DIGI- JA VÄESTÖTIETO-VIRASTO

Keinoja ja suosituksia turvata kriittisiä tietovarantoja, tietopalveluita ja tietojärjestelmiä

Tukimateriaali

20.12.2022

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Digitalisaation tukipalvelut ja yhteentoimivuus
/ Koivuoja Mervi (DVV)

20.12.2022

Tiivistelmä

Valtioneuvoston periaatepäätöksessä 2019 Suomen kyberturvallisuusstrategiasta on tunnistettu tarve kansallisen kyberturvallisuuden kokonaistilan parantamiseksi. Kyberturvallisuusstrategian pohjalta on laadittu kyberturvallisuuden kehittämisohjelma, jonka tavoite on luoda Suomeen kyberturvallisuuden ekosysteemi. Ekosysteemin kasvattamiseen pyritään neljällä pääteemalla, jotka ovat huippuluokan osaaminen, kiinteä yhteistyö, vahva kotimainen kyberturvateollisuus ja tehokkaat kansalliset kyberturvakyvykkyydet.

Kehittämisohjelman yhtenä alueena ja tavoitteena on digitaalisen yhteiskunnan keskeisten tietojen, tietovarantojen ja -palveluiden turvaaminen. Tavoitteen saavuttamisen mittariksi on määritetty: ”Tietovarannot, -palvelut ja -järjestelmät on tunnistettu ja niiden saatavuus ja turvallisuus on varmistettu koko elinkaaren ajan (kehitys, tuotanto, tuotannosta poisto)”.

Edellä mainittuun tavoitteeseen pääsemiseksi tässä työssä keskityttiin selvittämään Suomen olosuhteisiin sopivia laeissa esitettyjen vaatimusten täyttämiseksi parhaita käytäntöjä sekä koti- että ulkomaisista lähteistä. Käytännöt tiivistyvät tässä raportissa keinovalikoimiin ja suosituksiin, joiden pohjalta voidaan varmistaa ja turvata yhteiskunnan kannalta kriittiset tietovarannot, - palvelut ja -järjestelmät.

Keinovalikoimia ja suosituksia on kuvattu yleisinä periaatteina ja niitä on myös taulukoitu 1) strategista tasoa (valtionhallinto) sekä 2) operatiivista tasoa (hyvinvointialueet ja kuntasektori) painottaen. Lisäksi on huomioitava, että valtionhallinnon osalta säädösvalmistelu ja muu valtakunnallinen vastuu edellyttävät erilaisen lähestymistavan kuin mitä vastuut ovat esimerkiksi hyvinvointialueiden tai kuntasektorin toimijoilla. Operatiivisia asioita hoidetaan kuitenkin niin valtionhallinnossa kuin alue- ja paikallistasoilla tietovarantojen, tietopalveluiden sekä tietojärjestelmien elinkaaren hallinnassa.

Tämä työ suosituksineen on julkinen ja tarjoaa turvallisuudesta ja tietohallinnosta vastaaville työkaluja tietovarantojen, tietopalveluiden ja tietojärjestelmien toiminnan varmistamiseen, elinkaaren hallintaan sekä turvallisuuden kehittämiseen. Edellä mainitut asiat ovat, tai ainakin pitäisi olla, niiden omistajien tiedossa. Tässä esitetyt prosessit ja mallit mahdollistavat itsetarkastelun tai helpottavat tarkasteluun tarvittavan tuen määrittelyssä.

Digitalisaation tukipalvelut ja yhteentoimivuus
/ Koivuoja Mervi (DVV)

20.12.2022

Sisällysluettelo

Digitalisaation tukipalvelut ja yhteentoimivuus
/ Koivuoja Mervi (DVV)

20.12.2022

Keinoja ja suosituksia turvata kriittisiä tietovarantoja, tietopalveluita ja tietojärjestelmiä

Tässä raportissa on kuvattu keinoja kriittisten tietovarantojen, -palveluiden ja -järjestelmien saatavuuden ja turvallisuuden varmistamiseksi koko elinkaaren ajan. Johdanto luvussa on kuvattu selvityksen tausta, tavoitteet, määritelmät, rajaukset sekä lueteltu muut asiaan liittyvät selvitykset.

Toisessa luvussa on esitetty keinoja ja suosituksia yllä mainittujen tietoon liittyvien asioiden turvallisuuden kehittämiseksi. Lisäksi raportin lopussa on koonnos eri lähteistä kerätyistä dokumenteista, joita voidaan hyödyntää kyberturvallisuuden kehittämisessä ja toiminnan turvaamisessa.

Tässä esitettyjä keinovalikoimaa ja suosituksia voidaan hyödyntää esimerkiksi julkishallinnon digitaalisen toimintaympäristön strategisessa suunnittelussa, muutosjohtamisessa, elinkaaren hallinnassa, turvallisuuden kehittämisessä sekä riskienhallinnassa.

1 Johdanto

1.1 Tausta ja tavoitteet

Valtioneuvoston periaatepäätöksessä 2019 Suomen kyberturvallisuusstrategiasta on tunnistettu tarve kansallisen kyberturvallisuuden kokonaistilan parantamiseksi. Kyberturvallisuusstrategia liittyy yhteiskunnan turvallisuusstrategian (2017) ja EU:n kyberturvallisuusstrategian toimeenpanoon sekä niistä johdettuihin Kyberturvallisuuden kehittämisohjelman 2021 tavoitteisiin.[1]

Kyberturvallisuuden kehittämisohjelman tavoite on luoda Suomeen kyberturvallisuuden ekosysteemi. Ekosysteemin kasvattamiseen pyritään neljällä pääteemalla, joita ovat huippuluokan osaaminen, kiinteä yhteistyö, vahva kotimainen kyberturvateollisuus ja tehokkaat kansalliset kyberturvakyvykkyydet.[2]

Kehittämisohjelman toimeenpanosuunnitelmassa on tunnistettu 12 aluetta, joilla tavoitteeseen voidaan päästä. Yksi niistä on digitaalisen yhteiskunnan keskeisten tietojen, tietovarantojen ja -palveluiden turvaaminen (alue 11). Alueen teemana on tehokkaat kansalliset kyberturvakyvykkyydet ja niiden pohjalta johdettu kehittämistoimenpide on tunnistaa yhteiskunnan kannalta kriittiset tietovarannot, - palvelut ja -järjestelmät sekä varmistaa niiden toiminta ja turvallisuus (alue 11.1). Tavoitteiden saavuttamisen mittariksi on määritetty: ”Tietovarannot, -palvelut ja -järjestelmät on tunnistettu ja niiden saatavuus ja turvallisuus on varmistettu koko elinkaaren ajan (kehitys, tuotanto, tuotannosta poisto)”.[3]

Tämä toimeenpano-ohjelman osa keinovalikoimineen ja suosituksineen on laadittu Kyberturvallisuuden kehittämisohjelman 2021 alueen 11.1 osaksi. Tässä dokumentissa

[1] Kyberturvallisuuden kehittämisohjelma LVM 2021, s 7
[2] Kyberturvallisuuden kehittämisohjelma LVM 2021, s 10
[3] Kyberturvallisuuden kehittämisohjelma LVM 2021, Liite 1 s 31

esitellään laeissa esitettyjen vaatimusten täyttämiseksi Suomen olosuhteisiin sopivia parhaita käytäntöjä sekä koti- että ulkomaisista lähteistä. Käytännöt tiivistyvät tässä raportissa keinovalikoimiin, joiden pohjalta voidaan varmistaa ja turvata yhteiskunnan kannalta kriittiset tietovarannot, - palvelut ja -järjestelmät. Keinovalikoimat ovat taulukoitu 1) strategisella tasolla sekä 2) operatiivisella tasolla.

1.2 Määritelmiä

Tässä selvityksessä digitaalisella ekosysteemillä tarkoitetaan tietovarantojen, tietopalveluiden ja tietojärjestelmien muodostamaa kokonaisuutta.

Tietovarannolla tarkoitetaan loogista tiedoista koostuvaa omaisuutta, jota jokin taho hallinnoi.[4] Julkisessa hallinnossa tietovarannot ja niiden ylläpito on lainsäädännöllä säädelty ja pitänyt dokumentoida lain säätämällä tavalla muun muassa tietoaineistojen elinkaaren hallinnan näkökulmasta.

Tietopalvelua on esimerkiksi julkishallinnon järjestelmissä olevien asiakirjojen tai tietojen antaminen pyynnöstä tiedotusvälineiden, tutkijoiden, tilastolliseen tai kansalaisten käyttöön. Tietopalvelua voivat myös olla avoimen data julkaisu rajapinnan kautta, sähköisen tietopalvelun toteuttaminen, tilastojen julkaiseminen, viestintä ja aktiivinen uutisointi, joka on lähtöisin tiedon omistavan organisaation omista tarpeista.[5]

Tietojärjestelmiksi ymmärretään muun muassa tietojenkäsittely- ja tiedonsiirtolaitteista, käsittelysäännöistä, tiedoista ja tietoja käsittelevistä ihmisistä muodostuva kokonaisuus. Tietojärjestelmien tarkoitus on mahdollistaa, tehostaa tai helpottaa jotakin toimintaa.[6]

K3TTu on lyhenne seuraavista sanoista: K = **K**einoja, 3T = **T**ietovaranto, **T**ietopalvelu, **T**ietojärjestelmä ja Tu = **Tu**rvaaminen. Työssä käytetään edellä mainituin sisällöin 3T- ja 3TTu -lyhenteitä.

Strategisella tasolla tarkoitetaan johtotasoa, joka vastaa esimerkiksi lainsäädännön valmistelusta, suositusten laatimisesta, merkittävien resurssien varaamisesta ja suurten muutosten johtamisesta. Operatiivinen taso toteuttaa ja ylläpitää esimerkiksi tietovarantoja, tietopalveluita sekä tietojärjestelmiä.

---

[4] tietovaranto | TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma): ”Tietovaranto voi olla fyysisesti keskitetty tai hajautettu. Julkishallinnon tietovarantoja ovat esimerkiksi väestörekisteri, kiinteistörekisteri, säädöstietokokoelma, monet tilastot sekä kartta- ja paikkatietoaineistot. Myös yksityisillä yrityksillä on tietovarantoja, esimerkiksi asiakasrekisterejä”

[5] Tietopalvelu - Oikeusrekisterikeskus: Esimerkiksi ”Viranomaisten laatimat ja heidän hallussaan olevat asiakirjat ovat julkisia, ellei niitä ole lailla määrätty salaisiksi. Asiakirjajulkisuudesta säädetään julkisuuslaissa. Jokaisella on oikeus saada tieto mistä tahansa julkisesta viranomaisen asiakirjasta riippumatta siitä, onko hän asiassa asianosainen vai ei. Viranomainen voi harkintansa mukaan antaa tiedon myös asiakirjasta, joka ei vielä ole julkinen.”

[6] tietojärjestelmä | TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma): ”Järjestelmä, jonka tarkoitus on tietoja käsittelemällä palvella jotakin toimintaa. Tietojärjestelmän muodostavat tiedot ja niiden käsittelysäännöt, käsittelyn henkilö- ja laiteresurssit sekä tiedonsiirtolaitteet ja toimintaohjeet.”

Valtionhallinnolla tarkoitetaan tässä selvityksessä ministeriöitä ja virastoja. Alue- ja paikallishallinnolla tarkoitetaan perusteilla olevia hyvinvointialueorganisaatioita sekä nykyisiä kuntia ja kaupunkeja.

Osaamisen kehittäminen ja opettaminen erotetaan siten, että osaamisen kehittäminen on työelämässä tapahtuvaa valmentamista (aikuisopetusta ja -koulutusta, virtuaalisia kursseja, erilaisia organisaatioiden järjestämiä osaamisen kehittämiseen liittyviä toimia ja harjoituksia) ja opettaminen yliopistojen, ammattikorkeakoulujen ja ammattikoulujen tekemää työtä.

1.3 Rajaukset

Tässä selvityksessä käsitellään kyberturvallisuuden ekosysteemiä kansallisella tasolla. Yksittäiset organisaatiot voivat hyödyntää tuloksia omassa kyberturvallisuuden ekosysteemissään sen erityispiirteet huomioiden. Turvallisuussyistä tietojärjestelmiä ja niiden omistajia ei kerrota nimeltä. Toisaalta Suomessa olevien tietovarantojen, tietopalveluiden sekä tietojärjestelmien selvittäminen yksityiskohtaisesti olisi ollut työhön varatussa ajassa mahdoton tehtävä.

Tämä selvitys koskee kyberturvallisuuden kehitysohjelman kohtaa 11.1, jossa on keskitytty julkisen sektorin organisaatioihin. Selvitys on tehty julkisen sektorin organisaatioille, mutta selvityksen tuloksia voidaan hyödyntää myös yksityiselle sektorille. Toisaalta tekniikka ja prosessit ovat hyvin pitkälle samankaltaista, joten tämä työ on laite- ja prosessiriippumaton, oli kyseessä julkinen tai yksityinen sektori.

Selvitys pitää sisällään perusteltuja keinoja ja suosituksia, mutta ei välttämättä ota huomioon eri tietovarantojen, tietopalveluiden ja/tai tietojärjestelmien erityispiirteitä ja/tai yksityiskohtia.

1.4 Muut aiheeseen liittyvät työt

Tämän työn rinnalla on käynnissä Huoltovarmuuskeskuksen ja Kuntaliiton toimesta vastaava selvitys kriittisen infrastruktuurin kyberturvallisuuden tasosta. Lisäksi rinnalla on tehty tai tehdään muita kehittämisohjelman mukaisia selvityksiä.[6]

Lisäksi Valtiovarainministeriön Haukka-hanke sekä Digi- ja väestötietoviraston JUDO-hankkeen osat sisältävät tätä selvitystä tukevia asioita.[7] [8] Niin ikään useilla muillakin tahoilla on käynnissä vastaavia selvityksiä.

2 Keinoja ja suosituksia tietovarantojen, tietopalveluiden ja tietojärjestelmien tunnistamiseen ja turvaamiseen

Julkisella sektorilla on meneillään useita kehityshankkeita eri turvallisuuden alojen kehittämiseksi. Taustalla on myös vuosia kestänyttä työtä turvallisuuden ylläpitämiseksi ja parantamiseksi. Henkilöstön vaihtuvuus, tekniikan kehittyminen sekä viime vuosina

[6] Kyberturvallisuuden kehittämisohjelma LVM 2021 Kyberturvallisuuden kehittämisohjelma - Valto (valtioneuvosto.fi)
[7] Hankkeet | Digi- ja väestötietovirasto | Digi- ja väestötietovirasto (dvv.fi)
[8] JUDO-hanke, Väliraportti 2019-2021 (dvv.fi)

radikaalisti muuttunut maailman geopoliittinen tilanne on asettanut digitaalisen toimintaympäristön tarkastelut uuteen ja konkreettisempaan valoon. Koronapandemia sekä Ukrainan sota seurauksineen ovat olleet haasteellisia. Kriisien yllättävyys, kustannusrakenteiden muutokset, toimitusketjujen luotettavuus sekä energian saanti herättävät kysymyksiä digitaalisen toimintaympäristön resilienssistä.

Koko yhteiskunnan digitaalisen toimintaympäristön selkärangan muodostavat tietovarannot, tietopalvelut sekä tietojärjestelmät. Siksi niiden turvallisuuteen tulee kiinnittää huomiota koko niiden elinkaaren ajan. Tässä luvussa kiinnitetään huomiota keinoihin, joilla turvallisuutta voidaan kehittää ja ylläpitää. Turvaamiseen liittyvät kehityskohteet, keinot, perustelut ja suositukset on jaettu kahteen osaan eli strategiseen ja operatiiviseen tasoon.

Tarkastelussa on huomioitu haasteet, keinot, perustelut ja suositukset kunkin keinon osalta. Tässä työssä on kuvattu joitakin esimerkkejä, mutta keinojen ja suositusten valinta on kuitenkin tehtävä tapauskohtaisesti.

2.1 Lähestymistapa: elinkaari, turvallisuus ja 3T-kokonaisuus

Tässä työssä esitetty kokonaisuus voidaan hahmottaa alla esitetyn kuvan kautta.

Elinkaariajattelu koskee jokaista tietovarannon, tietopalvelun ja tietojärjestelmän omistajaa. Turvallisuustoiminnalla taataan jatkuvuus erilaisissa muuttuvissa tilanteissa kaikissa alla kuvatuissa tietoa koskevissa hallinta-alueessa.

Kuva: 3TTu -kokonaisuuden hahmottaminen ja sekä siinä olevat riippuvuudet

Digitaalisen ekosysteemin eri asioiden tunnistaminen ja ymmärtäminen on haasteellinen tehtävä, mutta se on välttämätöntä tieto-omaisuuden hallitsemiseksi. Yksi keino on jakaa asiat pienempiin osiin ominaisuuksien tunnistamiseksi. Kokonaisuus on todennäköisesti helpompi hallita, kun on selvitetty, mistä paloista ja millaisista keskinäisriippuvuuksista on kyse. Hallinnan haasteellisuutta lisää jatkuvat muutostarpeet, jolloin yhdenkin alueen muutoksen vaikutus voi heijastua koko ekosysteemiin.

Edellä mainitusta voidaan esimerkkinä mainita uusi tietojärjestelmä ja sen käyttöönotto. Ratkaistavia asioita ovat tällöin yleensä esimerkiksi edellisessä järjestelmässä

tuotettujen ja säilöttyjen tietojen (tietovaranto) yhteensopivuus uudessa tietojärjestelmässä, muutokset tietopalveluiden prosesseissa, turvallisuusratkaisut sekä koko muutoksen johtaminen ja käyttäjien kouluttaminen uuteen järjestelmään.

2.1.1 Elinkaarenhallinta

Kaikilla toiminnoilla ja tuotteilla on oma elinkaarensa. Yksi esimerkki havainnollistaa elinkaaren vaiheita on esitetty alla olevassa kuvassa. Keskittymällä elinkaaren suunnitteluun ja elinkaaren hallintaan, voidaan 3T turvallisuusrakennetta kehittää. Lisäksi hyvin tehdyt suunnitelmat mahdollistavat erilaisten riskien ennalta tunnistamisen ja turvallisen poistamisen.

Kuva: Kriittisten tietovarantojen, tietopalveluiden ja tietojärjestelmien elinkaaren hallinta (esimerkki)

Yleensä elinkaarien hallintaprosesseja on useita. Esimerkiksi jokaisella tietojärjestelmällä on usein oma elinkaari, josta julkishallinnossa yleensä vastaa nimetty omistaja. Yksi merkittävä haaste elinkaarenhallinnassa on eriaikaisuus ja keskinäisriippuvuus. Lisäksi tietovarantojen omistajuudessa saattaa olla puutteita.

Keskeisiä keinoja elinkaarien hallitsemiseksi on yhteistoiminta, keskinäinen viestintä, osaamisen kehittäminen, omistajuus, suunnittelu, seuranta, kypsyyksien arviointi, muutostarpeiden tunnistaminen, riskilähtöinen turvallisuusrakenteiden ylläpito ja kehittäminen sekä asioiden ennakointi.

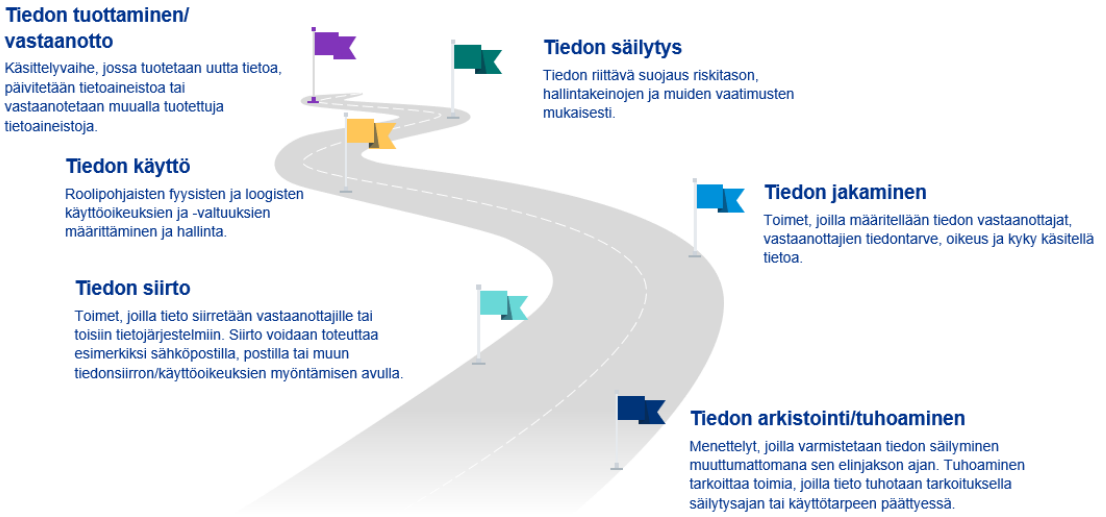
Seuraavissa alaluvuissa tarkastellaan elinkaarta 3T:n osalta. Lisätietoa ja tarkempia ohjeita elinkaaresta 3T:n osalta löytyy muun muassa tiedonhallintalautakunnan suosituskokoelmasta tiettyjen tietoturvallisuussäännösten soveltamisesta.[9]

2.1.1.1 Tietovarantojen elinkaari

Tiedon elinkaariajattelu perustuu tiedon riskilähtöiseen ja suunnitelmalliseen käsittelyyn ja hallintaan. Tiedon elinkaari alkaa tiedon vastaanottamis- tai tuottamisvaiheessa ja päättyy tiedon tuhoamiseen tai pysyvään säilyttämiseen. Täten tiedon elinkaari sisältää seuraavat vaiheet: tiedon vastaanottaminen tai tuottaminen, säilytys, käyttö,

[9] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta - Valto (valtioneuvosto.fi)

jakaminen, siirto, tuhoaminen tai arkistoiminen.[10] Tiedon elinkaarta havainnoidaan alla olevassa kuvassa.



Kuva: Tietoaineiston/tietovarannon elinkaariprosessi

Tiedon elinkaaren osalta tulee muistaa, että tietoja käsitellään eri tietojärjestelmissä ja sijainneissa, jolloin tiedolla voi olla oma elinkaarensa, mikä on usein pidempi kuin yksittäisen tietojärjestelmän elinkaari.[11]

Tietoturvallisuus on osa tiedon elinkaarta. Tiedon elinkaaressa tietoturvallisuus muodostaa kokonaisuuden, johon sisältyy tiedon luokittelu, riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien pohjalta ja tietoturvallisuustoimenpiteiden toteuttaminen. Tietoaineistoihin liittyviä riskejä tulee arvioida säännöllisesti tiedonhallintayksikössä tiedon koko elinkaaren ajan.[12]

2.1.1.2 Tietopalveluiden elinkaari

Koska tietopalveluita ovat esimerkiksi julkishallinnon järjestelmissä olevien asiakirjojen antaminen pyynnöstä tiedotusvälineiden, tutkijoiden, tilastolliseen tai kansalaisten käyttöön, tulee palveluprosessi kuvata sekä huomioida mahdolliset säädöksissä ja tietojenkäsittely-ympäristöissä tapahtuneet muutokset koko elinkaaren ajan.

Elinkaariajattelussa on lisäksi huomioitava, että tietopalvelua voivat myös olla tilastojen julkaiseminen, viestintä ja aktiivinen uutisointi, jotka ovat lähtöisin tiedon omistavan organisaation omista tarpeista. Tältä osin tietojen säilyttäminen sekä looginen viestintä seuraa tietopalveluprosessia koko tietoon liittyvän elinkaaren ajan. Tietopalveluiden elinkaari on havainnollistettu seuraavassa kuvassa.

[10] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta : Lautakunnat (valtioneuvosto.fi) s 13
[11] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta : Lautakunnat (valtioneuvosto.fi) s 13
[12] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta : Lautakunnat (valtioneuvosto.fi) s 13-14

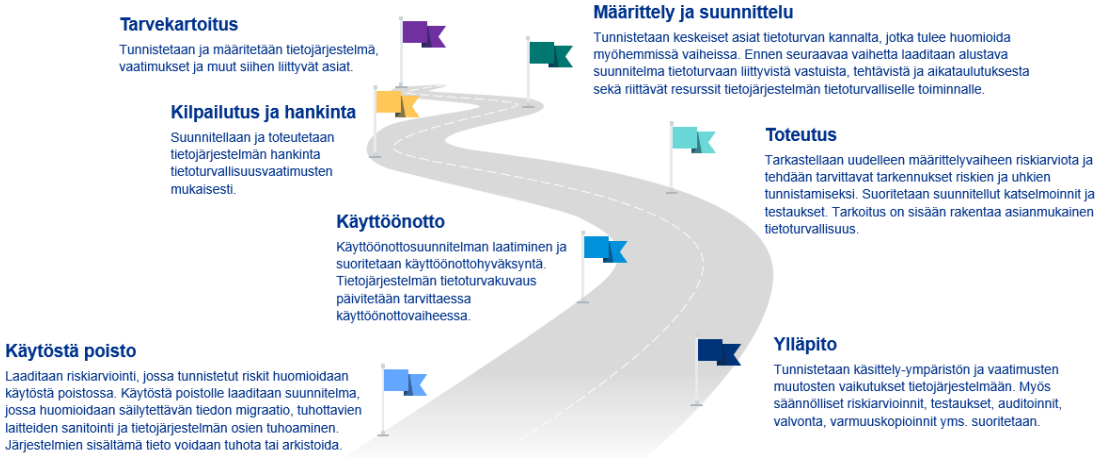
Kuva: Tietopalvelun elinkaariprosessi

Tutkimuksellisessa näkökulmassa tietopalvelun haasteeksi voi muodostua asiakirjaformaattien ja käytössä olevien tietojärjestelmien muutokset. Historiatieto saattaa kadota, vaikka se olisikin arkistoitu osana tietopalvelun tavoitteita.

2.1.1.3 Tietojärjestelmien elinkaari

Tietojärjestelmien elinkaariajattelu perustuu järjestelmässä käsiteltävien tietojen huomiointiin sekä järjestelmien riskilähtöiseen ja suunnitelmalliseen hallintaan tiedonhallintayksikössä. Tietojärjestelmän elinkaari alkaa tarvekartoituksesta ja päättyy järjestelmän käytöstä poistoon.

Täten tietojärjestelmän elinkaari sisältää seuraavat vaiheet: määrittely ja suunnittelu, kilpailutus ja hankinta, toteutus ja kehitys, käyttöönotto, ylläpito sekä käytöstä poisto.[13] Tietojärjestelmien elinkaarta havainnoidaan alla olevassa kuvassa.



[13] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta : Lautakunnat (valtioneuvosto.fi) s 22

Kuva: Tietojärjestelmän elinkaariprosessi

Tietojärjestelmien elinkaaressa tietoturva muodostaa kokonaisuuden, johon sisältyy riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimien toteutus. Tiedonhallintayksikön tulee varmistaa tietojärjestelmien tietoturvallisuus koko elinkaaren ajan tunnistamalla riskit ja määrittää tietoturvallisuustoimet riskiarvioinnin perusteella.[14]

2.1.2 Tietovarantojen, tietopalveluiden ja tietojärjestelmien hallinta

Digitaalisen ekosysteemin hallinta edellyttää tietovarantojen, tietopalveluiden sekä tietojärjestelmien hallintaa. Ne muodostavat kokonaisuuden, jossa tietovaranto on jonkin tahon hallinnoimaa loogista tiedoista koostuvaa omaisuutta.

Kuva: Tietovarantojen, tietopalveluiden ja tietojärjestelmien muodostama kokonaisuus

Usein kuvassa olevat alueet on omistajuus- ja vastuuosiltaan erotettu toisistaan. Tiedon hallinnan osalta yllä olevat alueet muodostavat prosessin. Ilman tietojärjestelmiä ei voida tuottaa ja varastoida tietoja tietovarannoksi ja ilman tietopalvelua sekä tietopalvelun periaatteita tietoa ei ole käytettävissä. Tietojärjestelmiä voi olla useita, samoin kuin niillä tuotetulla tiedoilla yhteisiä tai erillisiä tietovarantoja.

Keskeisiä tietojärjestelmien hallintakeinoja ovat tietojärjestelmäluettelot, tietojärjestelmien arkkitehtuurit, konfiguraatiotiedot, omistajat sekä riippuvuudet. Tietovarantojen hallintakeinoja ovat niin ikään luettelot, niiden omistajat sekä riippuvuudet. Tietopalveluiden hallintakeinoja voi olla prosessien tunnistaminen ja ylläpito. Tietopalvelut voivat olla osa viestintää, tietoihin liittyvää turvallisuusluokittelua sekä tietoihin liittyvää pääsyoikeuksienhallintaa.

Tietovarantojen luomisen ja tallentamisen sekä säilyttämisen ja arkistoinnin ja siitä tulevan tietopalvelun tulee aina perustua organisaation toiminnan luonteesta johtuvaan tarpeeseen sekä sääntelyyn.[15]

[14] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta : Lautakunnat (valtioneuvosto.fi) s 22
[15] Lausuntokierrokselta saatu palaute.

2.1.3 Turvallisuuden eri osa-alueet

Digitaaliseen toimintaympäristöön yhdistetään usein kyber-, tieto- tai digitaalinen turvallisuus sekä tietosuoja. Turvallisuuden osa-alueita on useita, joista alla olevassa kuvassa on yksi esimerkki. Siinä on myös huomioitu turvallisuusrakenteen kehittäminen, riskienhallinta sekä turvallisuusstrategia, -johtaminen ja -kulttuuri.

Kuva: Esimerkki kokonaisturvallisuuden osa-alueista ja turvallisuuden hallintamallista[16]

Turvallisuuden osa-alueista vastuita on yleensä jaettu eri tahoille. Tietovarantojen, tietopalveluiden ja tietojärjestelmien vastuutahojen olisi kuitenkin oltava aktiivisesti mukana kehittämässä turvallisuusrakenteita sekä huomioitava organisaation turvallisuustoiminnot omalla vastuualueellaan.

Turvallisuusrakenteiden laadun hallintakeinoja ovat testaaminen, arviointi tai auditointi. Julkishallinnon eri turvallisuuden laadunarviointikeinoja ovat esimerkiksi KATAKRI (turvallisuusjohtaminen, fyysinen turvallisuus, tekninen tietoturvallisuus), PITUKRI (turvallisuusjohtaminen, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, identiteetin ja pääsynhallinta, tietojärjestelmäturvallisuus, salaus sekä käyttöturvallisuus), JULKRI (hallinnollinen turvallisuus, fyysinen turvallisuus, tekninen turvallisuus,

[16] Mukailtu Elinkeinoelämän keskusliiton julkaisemasta rakenteesta.

varautuminen ja jatkuvuudenhallinta sekä tietosuoja), Kybermittari sekä erilaiset alan standardit. JULKRI on laajempi julkisen hallinnon arviointikehikko, joka sisältää PITUKRIN ja KATAKRIN kriteereiksi.[17] Edellä mainittujen keinojen kattavuutta ja soveltavuutta on syytä arvioida tapauskohtaisesti ja vertailla tässä luvussa esitettyyn esimerkinomaiseen kokonaisturvallisuuskuvaan.

Kyberturvallisuuden kehittämisen kymmenen askelta on esimerkinomaisesti esitelty seuraavassa kuvassa.

Kuva: Kymmenen askelta kyberturvallisuuteen[18]

Yhtenä tarkastelun keinona voidaan hyödyntää kansainvälisiä parhaita käytäntöjä. Kyberturvallisuuden osalta niitä löytyy runsaasti sekä Traficomin että erityisesti Yhdysvaltojen ja Ison-Britannian kyberturvallisuuteen keskittyneiden tahojen kotisivuilta. Tämän dokumentin lopussa on luetteloitu aiheeseen liittyviä hyödyllisiä linkkejä.

2.2 Keinoja ja suosituksia strategiselle tasolle

Strategisella tasolla tehdään koko yhteiskuntaa käsittelevät päätökset pitkän aikavälin vaikutuksineen. Yhtenä toimijana strategisella tasolla toimii valtionhallinto, mutta strategisen tason päätöksiä tehdään myös alue- ja paikallistasolla. Valtionhallintoon luetaan kuuluvaksi ministeriöt ja virastot sekä niiden tietovarannot, tietopalvelut sekä tietojärjestelmät. Valtionhallinnon vastuulla on kehittää lainsäädäntöä ja ohjeita sekä suorittaa valvontaa. Sen lisäksi se vastaa oman digitaalisen toimintaympäristön kehittämisestä ja ylläpidosta.

Strategisen toiminnan kehityskohtia ja keinoja kehittymiseksi on tunnistettavissa useita. Alla on listattu esimerkkejä keinoista, joita voidaan ryhmitellä seuraaviin luokkiin:

[17] Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) – Suositus ja kriteeristö (valtioneuvosto.fi) s 8

[18] 10 Steps to Cyber Security NCSC.GOV.UK

1 Elinkaaren hallinta

2 Opetus ja osaamisen kehittäminen ja sen koordinointi

3 Johtaminen; strateginen, operatiivinen ja muutosjohtaminen

4 Viestintä

Selvityksen mukaan strategisella tasolla on tehty runsaasti töitä kyberturvallisuuden parantamiseksi kehittämällä mm. säädöksiä, ohjeistusta, opastusta, tiedonvaihtoa, tietoisuutta, koordinointia, valvontaa, tukea, hankkeita, harjoituksia, yhteistyötä, huoltovarmuutta, tutkimusta sekä johtamista.

Samalla kun valtionhallinnon vastuun voidaan katsoa olevan yhteiskunnan elintärkeiden toimintojen turvaamisessa, suositellaan sen hoitavan kyberturvallisuuden osalta samoja operatiivisia asioita kuin muukin julkinen hallinto. Alue- ja paikallistasolla toiminta painottuu operatiivisten asioiden hoitamiseen heitä koskevien strategisten asioiden lisäksi.

Kehityskohteiden lisäksi on suositeltavaa kaikissa asioissa jo saavutettu taso yllä. Alla olevassa taulukossa on strategiselle tasolle suunnattuja

1. esityksiä kehityskohteista,
2. keinoja kehityskohteiden haasteiden minimoimisesta,
3. perusteluissa taustatietoa kehityskohteen haasteesta sekä
4. suosituksia esitettyjen keinojen käyttämisestä.

Kehityskohde	**Keino**	**Perustelu**	**Suositus**
Turvallisuustarkastukset	Auditoinnit ja riippumattomat tarkastukset. Niiden ohjeistaminen, vaatiminen ja toteutuksen valvonta. Katettava kaikki turvallisuuden osa-alueet. Standardien ja muutoin hyväksyttyjen menetelmien kehittäminen ja laajempi hyödyntäminen.	Organisaation toiminta saattaa olla monitahoista ja siksi kompleksista. Lisäksi ulkopuolinen voi nähdä asiat todellisimpina erilaisten teknisten ja toiminnallisten testien kautta.	Strategisten turvallisuutta koskevien tarkastusvaatimusten ja työkalujen jatkuva ylläpito ja kehittäminen. Tarkastuksien kannustimena voisi olla julkishallinnon ”kyberturvallisuusseteli”, johon strategisella tasolla varattaisiin rahoitus ja hakuperusteet. Valtionhallinnon operatiivisessa toiminnassa tulee toteuttaa tarkastuksia. Turvallisuustarkastuksissa hyödynnetään alan yrityksiä tai organisaatioita. Perusteena käytetään standardeja, yleisesti hyväksyttyjä menetelmiä (esimerkiksi KATAKRI, JULKRI, PITUKRI) tai teknisiä järjestelmiä. Järjestelmät ja menetelmät testataan teknisesti tai harjoituksissa.

Viestintä	Strategisen tason toimijan sisäisen ja ulkoisen viestinnän parantaminen ja selkeyttäminen normaalioloissa ja häiriötilanteissa. Terminologian yhtenäistäminen. Kyberturvallisuuden tietoisuuden lisääminen. Avoimuuden lisääminen.	Tämän selvitystyön haastatteluvaiheessa nähtiin erittäin tärkeäksi kehittää viestintää erityisesti organisaation sisällä ja sidosryhmissä.	Strategisen tason viestintäsuunnitelmien ja vaatimusten ylläpito ja kehittäminen koko julkishallinnolle. Valtionhallinnon keskinäinen viestintä suunnitellaan ja dokumentoidaan, miten viestintää tulee toteuttaa riittävällä tarkkuudella eri kohderyhmissä (omat työntekijät, sidosryhmät, asiakkaat). Testataan suunnitelma valmentamalla ja harjoituksissa sekä ylläpidetään sitä säännöllisesti. Mukana toiminnan kehittämisessä tulisi olla organisaation johto (johdon sitouttaminen). Viestinnän tehostaminen tuottamalla julkaisuja vähintään kolmella kielellä (suomi-ruotsi-englanti).
Osaamisen kehittäminen	Alan oppilaitosten ja työnantajien yhteistyön kehittäminen valtionhallinnon tasolla ja siten lähentää opetuksen ja yhteiskunnan tarpeita. Aikuisopetuksen lisääminen verkkokursseilla, tutkinnoilla (oppilaitoksista saatavat pätevyydet sekä sertifikaatit), valmennuksilla ja harjoituksilla.	Oppilaitosten opetus on korkealaatuista, mutta sitä vaivaa opettajapula ja oppilaitosten ja yhteiskunnan odotusten epätasapaino.	Alaan liittyvää yhteistyötä tulee koordinoida enemmän ja laatia selvityksiä todellisista tarpeista. Oppilaitosten opetusohjelmien tarkastaminen tehtyjen selvitysten pohjalta. Aikuisopetukseen tulisi varata resursseja ja pyrkiä antamaan opetusta ja tutkintoja (ml erilaiset sertifikaatit) eri kielillä (vähintään suomi-ruotsi-englanti. Nyt esimerkiksi suurin osa tietoturva-alan sertifikaateista on tehtävissä vain englanniksi). Lisäksi suositellaan verkostoitumista, yhteisen osaamisen kehittämistä osallistumalla esimerkiksi VAHTI- ja/tai ISAC-toimintaan sekä seuraamalla ilmaisia kyberturvakatsauksia asiantuntijoille ja johdolle.
Toimintaympäristö (sekä kokonaisympäristö että digitaalinen ympäristö)	Toimintaympäristön analysoinnin lisääminen mm huomioiden arkkitehtuurityö strategisella tasolla sekä uhkat ja riskit. Kokonaisanalyysi voidaan tuottaa useasta toimintaympäristöstä. Yksi niistä voi olla	Organisaatioiden sisäisen ja ulkoisen toimintaympäristön tunteminen koettiin selvitysten perusteella vaihtelevaksi. Toimintaympäristön tunteminen luo perustan tehokkaalle häiriön- sekä muutosten hallinnalle. Osa uhkista (valtiolliset ihmisperäiset) ovat	Yksi suositus on lisätä arkkitehtuuriopetusta oppilaitoksissa sekä aloitteleville että jo työelämässä oleville. Lisäksi on suositeltavaa tehdä toimintaympäristön analysointia alaan perehtyneiden asiantuntijoiden avustamana. Analysoinnin tulisi olla jatkuvaa. Lisäksi toimintaympäristöä tulisi

	digitaalinen toimintaympäristö.	julkishallinnolle yhteisiä, joten niiden keskitetty seuraaminen ja toiminnasta raportointi parantaisi merkittävästi toimintaympäristön tuntemusta ja riskien hallintaa.	katsoa laajemmin kuin vain oman organisaation lähistöltä.
Tilannetietoisuus	Strategisen tason tilannetietoisuuden tuottaminen. Perusteiden tuottaminen julkisen sektorin toimijoille koskien teknistä valvontaa, tietoa haavoittuvuuksista sekä häiriönhallintaa. ISAC-toiminnan laajentaminen.	Tilannetietoisuus perustuu saatavaan tilannekuvaan. Strategisella tasolla tilannetietoisuus on kohtalainen, mutta yhtenäistä ja riittävää kuvaa pidetään kehittämisen arvoisena. Tällä hetkellä strategisella tasolla tilannekuvaa tuotetaan mm. Valtioneuvoston kansliassa, Suojelupoliisissa ja Kyberturvallisuuskeskuksessa. Tilannetietoisuuteen liittyvä tieto ei tämän selvityksen mukaan kuitenkaan koettu olevan riittävän hyvin saatavissa esimerkiksi kuntasektorilla. Haasteeksi nähtiin erityisesti valtiollisten kybertoimijoiden tietojen saanti.	Riittävän tilannetietoisuuden kehittäminen saattaisi olla mahdollista lisäämällä eri hallinnonalojen välistä yhteistyötä ja selkeyttämällä, minkä tasoista tilannekuvaa kukin tuottaa ja mitä voisi muille tarjota sekä itse tarvita. Liian yksityiskohtaista vaatimusta tilannekuvan yksityiskohdista tulisi strategisella tasolla välttää. Lisäksi valtionhallinnon operatiivisessa toiminnassa suositellaan verkostoitumista, yhteisen osaamisen kehittämistä osallistumalla VAHTI-toimintaan ja/tai seuraamalla ilmaisia kyberturvakatsauksia asiantuntijoille ja johdolle.
Johtaminen	Strategisella tasolla pitkän aikavälin johtaminen toteutetaan strategioiden kautta. Se tuotetaan kehittämällä strategisen tason suunnittelua ja ohjeistusta, muutosten hallintaa sekä yksinkertaistamalla ja selkeyttämällä vastuujakoa. Monihäiriötilanteessa nopeiden ratkaisuiden kykyjen lisääminen.	Strategioiden tunteminen, etäisyys ja kattavuus vaihtelevaa. Erityisesti valtionhallinnon toiminnan siiloutuminen vaikeuttaa toiminnan priorisointia erityisesti laaja-alaisen häiriötilanteen hallinnassa. Mikäli samaa alustaa tai palvelun toimittajaa hyödyntää usea tietovarannon ja/tai tietojen omistaja, voi toipuminen monihäiriötilanteessa tulla haasteelliseksi. Alustan tai palvelun toimittajan kyky arvioida eri toimintojen prioriteettia voi olla mahdoton tunnistaa. Lisäksi toimintaympäristössä vallitseva tilanne	Strategioiden tuntemisen lisääminen ja konkretisointi, jotta strategia muuttuu käytännön toiminnan tavoitteeksi. Tälle suositellaan asettamaan mittari, jonka toteutumista seurataan tietoon perustuvalla päätöksenteolla ja kehittämistä varten. Päätöksen kyvyn ja johtamisen joustavuuden ja valtuutuksen lisääminen on suositeltavaa. Usean toiminnan kyberhäiriötilanteet ovat yleensä yllättäviä, jolloin valtionhallinnossa tulisi olla päättäjä, jolle tuotetaan riittävä tilannetietoisuus vallitsevasta tilanteesta palveluiden prioriteetin määrittämiseksi ja toiminnan johtamiseksi. Valtuudet ja vastuu tulisi olla

		voi olla ennalta aavistamaton, jolloin etukäteen tuotettu prioriteettisuunnitelma ei ole enää kurantti.	selkeämmin määritetty säädöspohjaisesti.
(Huolto)varmuus	Strategisen tason (huolto)varmuusvaatimusten kehittäminen. Tietoliikenneyhteyksien ja tietovarantojen kahdennukset, hajauttaminen, segmentointi sekä varautuminen (jatkuvuus- ja valmiussuunnittelu) sekä suunnitelmien testaaminen ovat resilienssi perusta.	Eri selvitysten perustella on jäänyt vaikutelma, että varautumisessa on kehittämisen varaa vaatimuksissa ja niiden noudattamisessa niin teknisellä kuin toiminnallisella alueella.	Tietovaranto- tietopalvelu-, tietojärjestelmä ja tietoliikennearkkitehtuurin laatiminen ja ylläpito valtionhallinnon toimintoihin. Suunnitteluperusteet muulle julkishallinnolle. Varautumisen suunnittelun toteuttaminen ja ylläpito (harjoittelu). Tarvittaessa ulkoisten asiantuntijoiden hyödyntäminen.
Omatoimisuus	Itsearviointi, testaaminen	Itsearvioinnin työkaluja on kehitetty viime vuosina, mutta niiden hyödyntämistä vaikuttaisi hidastavan resurssipula sekä viestinnän puute (mm. käsitteet) sekä rohkeus testata toimintoja.	Itsearvioitiprosessin kehittäminen avustamalla ensimmäisessä arvioinnissa. Työkalujen ohjeistuksen kehittäminen ja/tai hyödyntäminen esimerkiksi harjoituksissa.
Säädökset	Kehitysohjelmat ja -rahoitus, säädösten sisältö	Yksi julkisen hallinnon suurimmista haasteista on resurssien puute (taloudelliset, henkilöstö ja/tai osaaminen). Säädösten määrän lisääntymisen koettiin syövän jo olemassa olevia resursseja ja kokonaisvaltaisen vaatimusten tason koettiin kasvavan hallitsemattomasti.	Uusien säädösten keskinäisten vaikutusten kokonaisarviointi ennen laatimista. Resurssit tulisi ottaa huomioon erilaisten kehitysohjelmien kautta ja huomioida riittävän pitkät siirtymäajat.
Työkalujen hyödyntäminen	Katakri, julkri, pitukri, standardit, kybermittari sekä erilaiset DVV:n tuottamat työkalut (esim. kriittisten kohteiden tunnistaminen, arkkitehtuuri ja kokonaiskuva)	Erilaisia työkaluja on kehitetty viime vuosina, mutta niiden hyödyntämistä vaikuttaisi hidastavan resurssipula, viestinnän puute (mm. käsitteet) ja virallisesti hyväksyttyjen arviointiorganisaatioiden vähyys. Teknisen ja toiminnallisen kehityksen myötä osaamisen kehittäminen	Ohjeiden ja standardien päivittäminen. Viestinnän lisääminen. Harjoitusten järjestäminen.
Tukipalvelut	Ohjeet, HelpDesk-toiminta, yhteiset hankkeet	Tietopalveluissa tunnistetaan olevan tukipalveluita, mutta prosessi	Tukipalveluiden käyttäjäystävällisyyden lisääminen sekä tukipalveluiden osaamisen

		koettiin hankalaksi ja tuen saanti puutteelliseksi.	kehittäminen. Palveluvasteen ajan lyhentäminen.
Tekniset toimet	Keskittäminen, segmentointi, varmentaminen	Resurssipula nähtiin ongelmaksi erityisesti pienissä organisaatioissa teknisen ylläpidon osalta.	Suurilla keskityksillä voidaan toiminnot hoitaa pienemmillä resursseilla ja oikeilla segmentoinneilla suurten keskittymien turvallisuus taata riittävällä tasolla. Tekoälyn hyödyntäminen tietomassan louhinnassa sekä alustavassa analysoinnissa.
Verkoston rakenne	Verkoston rakenteen tunnistamiseen liittyvät strategisen tason vaatimusten päivittäminen ja niistä viestiminen (arkkitehtuuri, sopimukset, toimitusketjut, riippuvuudet, omistajuus, kriittiset pisteet, pilvipalvelut)	Verkostojen rakenne tunnetaan tämän selvityksen mukaan vaihtelevasti. Ymmärrys rakenteesta lähtee arkkitehtuurista, jonka tilanne oli vaihteleva ja odotukset vaihtelivat oman ja ulkoisen vastuun osalta. Näkymä ulkopuoliseen palvelutoimittajaan koettiin heikoksi.	Ulkopuolisten asiantuntijoiden hyödyntäminen. Palvelusopimusten kattavuuden tarkastaminen jo laadintavaiheessa kattavuuden huomioiminen.
Elinkaari	Suunnittelu, toteutus, ylläpito, poistaminen, dokumentaatio	Elinkaaren alkuvaihe aina ylläpitoon saakka vaikuttaa olevan hyvin hoidossa. Loppuvaihe ei välttämättä niin hyvin.	Elinkaariosaamisen lisääminen. Palvelumuotoiluajattelun ohjeistaminen strategisella tasolla sekä valtionhallinnon keskitetyissä palveluissa sen lisääminen.
Tiedonhallinta	Tiedot, tietovarannot, tietopalvelut, kohdennetut selvitykset (yksi asia keskiössä kerrallaan)	Tieto on organisaation tärkein voimavara, mutta usein huomio vaikuttaa kiinnittyvän liiaksi yksittäisen teknologian toimivuuteen.	Tietovarantoja (esim. avointa dataa) koskevaa arkkitehtuuria strategisella tasolla tulisi ylläpitää ja viestiä olemassa olevien tietovarantojen suomista mahdollisuuksista.
Turvallisuusrakenteet	Esim. Katakrin mukaan, eli johtaminen, fyysinen, tekninen, kyberuhkat (haittaohjelmat/tietomurrot/APTt/ /informaatiovaikuttaminen/...)	Turvallisuuden osa-alueiden tarkastukset ja ylläpito on toteutettu vaihtelevasti tai niihin ei ollut näkymää. Uhkatekijät, erityisesti valtiolliset tahot (mm. APT:t), koettiin valtionhallinnon tarjoamaksi palveluksi. Esimerkiksi kuntasektorilla tähän ei nähty olevan mahdollisuuksia ja toisaalta esimerkiksi APT-toimijat ovat koko yhteiskunnan kannalta samoja toimijoita.	Tarkastukset turvallisuuden eri osa-alueilla. Kansallisen uhka-arvion tuottaminen ja hyödyntäminen sekä operatiivisen tason tuki.

Varmentaminen	Dokumenttien varmentaminen tulisi tehdä vähintään kahdentamalla, hajauttamalla, on- ja offline ratkaisuilla. Joissakin tapauksissa paperiset arkistot saattavat edelleen tulla kyseeseen. Varmentamiseen liittyvä ohjeistus ja säädökset ovat strategisen tason toimia.	3T ympäristöt sisältävät runsaasti arkaluontoista ja esimerkiksi toipumisen kannalta tärkeää tietoa. Eri tapauksissa on käynyt ilmi, että vakavan kyberhyökkäyksen kohteeksi joutunut organisaation on saanut palautettua toimintansa online-ratkaisuilla, mutta on myös tapauksia, joissa varmennukset ovat saastuneet hyökkäyksen seurauksena käyttökelvottomiksi.	Jokaisen organisaation tulisi tunnistaa, mitä tietoa tarvitaan kyberhyökkäyksestä palautumiseen ja toiminnan jatkamiseen. Kun edellä mainittu analysointi on tehty, on mahdollista määrittää prosessien ja tietoaineistojen varmentaminen. Pilvipalveluihin sijoitettu tieto voi olla useassa paikassa ympäri maailmaa, ja se voi olla hyvä asia. Palautuminen riippuu kansainvälisten tietoliikenneyhteyksien toimivuudesta. Joissakin kriittisten tietojenhallintatilanteissa voi olla hyödyllistä pitää vähintään varmennukset kotimaassa.
Parhaiden käytäntöjen hyödyntäminen	Julkisen materiaalin ”kampaaminen”, oman toimintaympäristön analysoiminen, asiantuntijoiden käyttö (omat tai ulkopuoliset). Käsitteiden määrittäminen, käännöstyöt ja lopputulosten käyttäjäystävällisyys	Tietovarantojen, tietopalveluiden ja tietojärjestelmien turvaamisen osalta on saatavissa runsaasti informaatiota ja parhaita käytäntöjä. Saatavan tiedon määrä nähdään kuitenkin vaikeaksi löytää ja tunnistaa se sopivaksi omaan toimintaan liittyen. Strategisella tasolla on otettava huomioon koko yhteiskunta sekä oman toiminnan kannalta tuotetut palvelut	Taustamateriaalin etsiminen ja sen priorisointi. Materiaalin jakaminen strategiseen koko yhteiskuntaa koskettavaan toimintaan sekä oman toiminnan kannalta tärkeisiin asioihin. Suositeltavaa myös käsitteiden määrittäminen ja ylläpito. Apuna voi käyttää oppilaitosten ja alan selvitystöitä tekevien organisaatioiden tutkimusresursseja.

2.2.1 Kehityksen kohteena elinkaarenhallinta

K3TTu- elinkaarenhallinnassa noudatetaan pitkälti samoja periaatteita kuin minkä tahansa tuotteen tai palvelun elinkaaressa. Merkittävä ero kuitenkin koskee asian virtuaalisuutta sekä immateriaalista osuutta. Vaikka mekaanisteknisiä alustoja voidaan kierrättää, on huomioitava mahdolliset arkaluontoiset tiedot ja niiden poistaminen kierrätykseen menevästä materiaalista. Tietopalveluissa nousee keskeiseksi kysymykseksi esimerkiksi uudet prosessit ja henkilöstön käyttö. Tietovarannoissa tulee huomioida niiden käytön jatkuvuus uudella alustalla. Lisäksi kaikkien edellä mainittujen keskinäiset riippuvuudet tulee huomioida.

Elinkaaren tehokas hallinta edellyttää jatkuvaa riskipohjaista seurantaa ja arviointia. Strategisen tason ohjeistuksessa voisi selkeämmin tuoda esille, miten elinkaarimallit

voisivat soveltua tietovarantojen, tietopalveluiden ja/tai tietojärjestelmien turvallisuuden hallintaan.

Elinkaarisuunnitelmat voidaan tehdä jokaiselle edellä mainituille (K3TTu) erikseen, jotta perusteet riskien, muutosten ja häiriöiden hallintaan ovat olemassa.

2.2.2 Kehityksen kohteena opetus ja osaamisen kehittäminen

Opettaminen on yliopistojen, ammattikorkeakoulujen ja ammattikoulujen tekemää työtä ja osaamisen kehittäminen on työelämässä tapahtuvaa valmentamista.

2.2.2.1 Opettaminen

Tietojärjestelmien opetuksella, kuten koodaamisella ja teknisellä kehityspuolella on jo perinteitä. Samoin on erilaisia tietovarantojen käyttöä koskevaa opetusta ja tietopalveluiden tuotantoa.

Kyberturvallisuutta opetetaan vain muutamassa korkeakoulussa omana opetusohjelmanaan, kuten Kaakkois-Suomen ammattikorkeakoulussa ja Jyväskylän yliopistossa. Yksittäisten kurssien tai opintokokonaisuuksien tarjonta kyberturvallisuudesta on laajempaa ja ollut kasvussa.

Kyberturvallisuuteen liittyvä opetustarjonta käsittelee teknistä osaamista ja pienemmissä määrin hallinnollista osaamista. Selvityksen mukaan työelämän odotukset ja oppilaitosten tarjonta eivät kuitenkaan kohtaa kyberturvallisuuden alalla. Alan opetus on melko nuorta ja alaa vaivaa myös opettajapula.[19]

Valtionhallinnossa voisi lisätä turvallisuusalan oppilaitosten ja työnantajien yhteistyötä koordinoimalla alaan liittyvää yhteistyötä sekä laatia selvityksiä todellisista tarpeista.

Yksittäisiä kyberturvaa käsitteleviä kursseja tai opintokokonaisuuksia olisi myös hyvä voida liittää osaksi muiden alojen koulutuksia, jotta kyberturvaosaamisen perustaso kehittyisi kaikilla aloilla.

Opettajapulaan on vaikea löytää nopeaa ratkaisua muutoin kuin rekrytoimalla suoraan valmistuneita tai hankkimalla osaamista ulkomailta.

2.2.2.2 Osaamisen kehittäminen

Työelämässä olevien valmentaminen on haaste kyberturvallisuuden alalla. Aikuisopetukseen tulisi varata resursseja ja pyrkiä antamaan opetusta ja tutkintoja, esimerkiksi erilaisia sertifikaatteja, eri kielillä (vähintään suomi-ruotsi-englanti. Nyt esimerkiksi suurin osa tietoturva-alan sertifikaateista on tehtävissä vain englanniksi).

Aikuisopetuksen ja osaamisen kehittäminen on myös niin ikään ollut kasvussa viime vuosikymmenien aikana. Myös tähän liittyen osaamisen kehittämisen tulisi vastata työelämän tarpeisiin.

[19] Tietoturva-alan opiskelijoita ei valmistu riittävästi eikä koulutus vastaa työelämän tarpeita, kertoo yliopistotutkimus (yle.fi):

Aikuisopetutusta voidaan lisätä verkkokursseilla ja erilaisilla tutkinnoilla, kuten oppilaitoksista saatavilla pätevyyksillä sekä sertifikaateilla, valmennuksilla ja harjoituksilla. Kurssien suorittamisesta ja ylläpidosta voisi olla myös joku kannustin, kuten pieni palkanlisä.

Aikuisopetusta voisi lisätä myös muilla aloilla kuin kyberturvallisuuden alalla, sillä kyberturvallisuus on tänä päivänä osa lähes kaikkia aloja. Tämä lisäisi yhteiskunnan turvallisuutta.

Osaamisen kehittäminen on elinikäinen prosessi. Useimmat julkisen sektorin organisaatiot järjestävät työntekijöilleen lisäkoulutusta ja perehdytystä. Oppilaitoksissa järjestetään erilaisia kursseja täydentämään osaamista, mutta tämän selvityksen perusteella vaikuttaa siltä, että organisaatioille jää liikaa vastuuta järjestää täydentävää henkilöstökoulutusta.

2.2.3 Kehityksen kohteena johtaminen

Strategisella tasolla johtaminen jakautuu kolmeen osaan: strateginen, operatiivinen ja muutosjohtaminen.

2.2.3.1 Strateginen johtaminen

Erityisesti valtionhallinnon tasolla korostuu strateginen johtaminen. Se on pitkän aikavälin johtamista strategioiden kautta, kuten kehittämällä strategisen tason suunnittelua ja ohjeistusta, muutosten hallinnan kehittämistä sekä vastuukysymysten yksinkertaistamista. Lainsäädäntötyö ja erilaiset ohjeet ovat keskeinen osa strategista johtamistoimintaa.

Myös alue- ja paikallistasolla strateginen johtaminen tulee ottaa huomioon. Vaikutusmahdollisuuksia voidaan käyttää muun muassa lakien valmisteluun ja ohjeiden laatimiseen omien strategisten johtamistavoitteiden ohella.

Eri strategiat saatetaan kokea etäisiksi ja huonosti tunnetuiksi. Yhtenä kehityskeinona voisi olla strategioiden konkretisointi ja tuntemuksen lisääminen viestinnän keinoin.

Eräät 3T toiminnot ovat strategisesti tärkeitä, mutta niiden priorisointi monihäiriötilanteessa voi olla haastavaa vaikutusten laajuuden, laadun ja keston vuoksi. Oman haasteen asiaan tuo 3T-ympäristöjen omistajuus. Jokaiselle omistajalle oma toiminta on tärkeää ja kokonaisuuden kannalta objektiivisen palautusoimia koskevien toimenpiteiden määrittäminen vaikeaa. Asiaa voidaan kehittää lisäämällä päätöksentekokykyä, mutta se edellyttää säädöspohjaista valtuutta.

2.2.3.2 Operatiivinen johtaminen

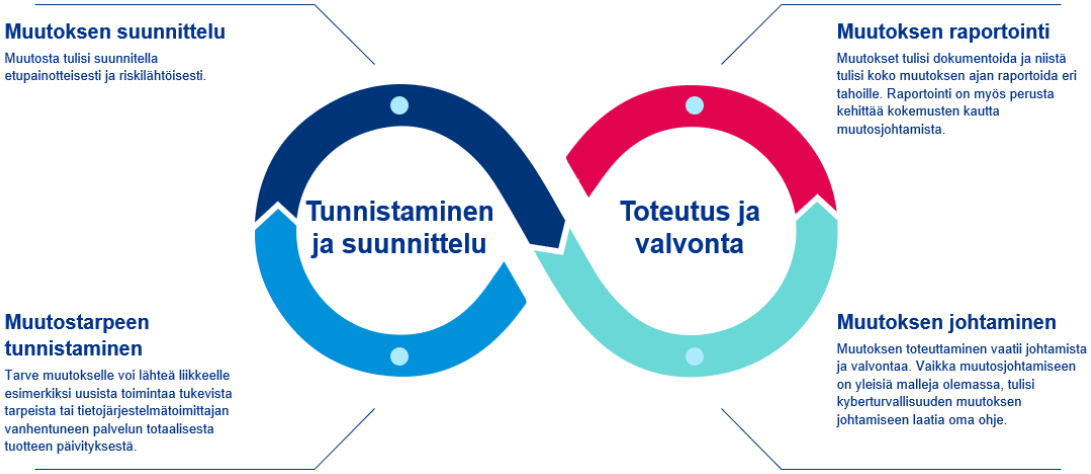
Yhtenä haasteena on tunnistettu eri virastojen välisten asioiden prioriteettilistojen tekeminen. On koettu haasteelliseksi tunnistaa, minkä hallinnonalan toiminta on monihäiriötilanteessa tärkeämpää kuin toisen. Lisäksi prioriteetti saattaa vaihdella häiriötilanteen laajuuden ja laadun vuoksi.

Monihäiriötilanteen toipumiseen liittyvä johtaminen on usein operatiivista johtamista. Sitä saatetaan joutua tekemään myös strategisella tasolla. Tällöin päätöksentekokyvyn ja johtamisen joustavuuden ja valtuutuksen lisääminen on suositeltavaa. Usean

toiminnon kyberhäiriötilanteet ovat yleensä yllättäviä, jolloin valtionhallinnossa tulisi olla päättäjä, jolle tuotetaan riittävä tilannetietoisuus vallitsevasta tilanteesta palveluiden prioriteetin määrittämiseksi ja toiminnan johtamiseksi. Valtuudet ja vastuu tulisi olla selkeämmin määritetty säädöspohjaisesti.

2.2.3.3 Muutosjohtaminen

Kyberturvallisuuden alalta ei ollut tunnistettavissa alaan liittyvää muutosjohtamisen ohjetta tai mallia. Sellaista ei ollut tunnistettavissa myöskään kansainvälisiltä sivuilta.



Kuva Esimerkki muutoksen johtamisesta

Muutosjohtamisen ohjeistuksen tai oppaan **kyberturvallisuuden tai kyberturvallisuuskulttuurin muutosten** osalta voisi ottaa huomioon tietovarantojen, tietopalveluiden ja tietojärjestelmien turvaamisen. Kuvassa on yleinen esimerkki muutosjohtamisen jatkumosta. Lisäksi muutosjohtamisen yksi keskeinen kysymys on itse muutokseen liittyvien riskien hallinta.

2.2.4 Kehityskohteena viestintä

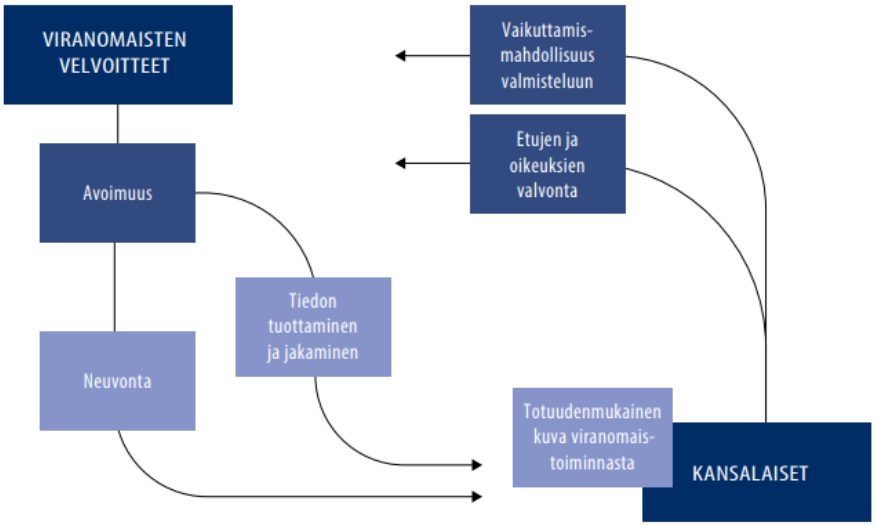
Viestintää voidaan pitää yhtenä johtamisvälineenä. Strategisen tason toimijan keinoina nähtiin sisäisen ja ulkoisen viestinnän parantaminen ja selkeyttäminen normaalioloissa sekä häiriötilanteissa. Viestinnän vastuiden jakaminen ja selkeyttäminen nähtiin tähän työhön liittyvän selvityksen perusteella kehittämiskohteeksi. Lisäksi viestinnän haasteena on kilpajuoksu huhuja ja muuta väärää informaatiovaikuttamista vastaan.

Sisäisen viestinnän kehittämiskeinoja voivat olla esimerkiksi erilaiset työryhmät, tietoiskut, harjoitukset ja intranet-tyyppiset kotisivut. Selvityksen aikana ilmeni, että organisaatioissa saatettiin tunnistaa taho, joka tuntee kysyttyjä asioita, mutta yksityiskohdista ei ollut riittävää tietoa. Tiedon käsittelyoikeuksien osalta tulee olla huolellinen, mutta riittävä avoimuus varmistaisi toiminnan aloittamisen esimerkiksi häiriötilanteissa.

Viranomaisten keskinäinen sekä sidosryhmien välinen viestintä on korostunut. Aiheesta on laadittu erilaisia ohjeita ja viestinnän tärkeyttä painotetaan myös palvelusopimuksissa. Tämän selvityksen aikana viestintä nähtiin hieman jälkipainotteisena sekä määrältään vaatimattomana. Esimerkiksi informaatiohäirinnän ja erilaisten

kybervaikutusten määrä on lisääntynyt ja niiden hallinnassa painottuu ennaltaehkäisevä ja ennakoiva viestintä.

Ulkoinen viestintä kohdistuu viranomaiskentässä pääasiassa kansalaisiin. Viestinnän ajoitus ja todenmukaisuus ovat erittäin tärkeitä. Ulkoisessa viestinnässä painottuu informaatiovaikuttamisen riskit, joihin varautumisella on mahdollista suojautua. Alla olevassa kuvassa on kuvattu ulkoisen viestinnän periaatteita.



Kuva: Ulkoisen viestinnän periaatteet[20]

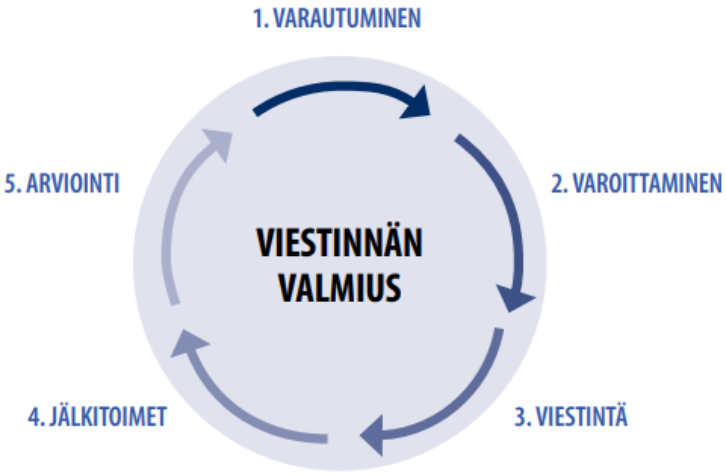
Viestinnän keinoja voidaan hyödyntää siten, että suunnitellaan ja dokumentoidaan, miten viestintää tulee toteuttaa riittävällä tarkkuudella eri kohderyhmissä (omat työntekijät, sidosryhmät ja asiakkaat). Suunnitelmat viestitään ja testataan valmentamalla sekä harjoituksissa, ja ylläpidetään niitä säännöllisesti. Toiminnan kehittämisessä pidetään organisaation johto mukana.

Viestintää voidaan tehostaa tuottamalla julkaisut vähintään kolmella kielellä (suomi-ruotsi-englanti). Myös terminologian yhtenäistäminen on yksi keino yhdessä kyberturvallisuuden tietoisuuden ja avoimuuden lisäämisen kanssa.

Kriisi- ja häiriötilanteissa viestintä on keskeinen osa johtamista. Tällaisessa tilanteessa korostuu tiedonkulku ja yhteistyö sekä oikea-aikainen ja luotettava viestintä.[21] Viestinnän parantamista voidaan kehittää laatimalla erilaisia suunnitelmia (esimerkiksi häiriötilanne- ja kriisiviestintäsuunnitelmat), keinoja ja malleja etupainotteisesti. Sitä voidaan kutsua valmiudeksi, jonka vaiheita on kuvattu alla olevassa kuvassa.

[20] Valtionhallinnon tehostetun viestinnän ohje – Viestintä normaalioloissa ja häiriötilanteissa (valtioneuvosto.fi) s 12

[21] Valtionhallinnon tehostetun viestinnän ohje – Viestintä normaalioloissa ja häiriötilanteissa (valtioneuvosto.fi) s 16



Kuva: Viestinnän valmius ja sen jatkuva kehittäminen[22]

Viestinnän prosessi voidaan pohtia siten, että tunnistetaan riskejä. Niiden kautta voidaan laatia mahdollisia skenaarioita ja siten antaa ennakkovaroituksia. Viestintä on oltava tosiasioihin perustuvaa. Viestinnän vaikutuksia tulee arvioida ja kehittää siten viestintää.

2.3 Keinoja ja suosituksia operatiiviselle tasolle

Operatiivisen tason toimintaa on valtionhallinnossa sekä alue- ja paikallistasolla. Alue ja paikallistaso muodostuu hyvinvointialueista ja kuntasektorista. Usealla kunnalla on viimeisen 15 vuoden aikana tapahtunut merkittäviä muutoksia kuntien yhdistymisen myötä ja yhdistymisprosessia on mahdollista jatkaa.[23]

Erityisesti vuoden 2022 tilannetta kuitenkin kuvaa hyvinvointialueiden perustamiseen liittyvä muutosprosessi. Hyvinvointialueiden organisointi on suunnitteluvaiheessa ja tuotantovaihe alkaa 1.1.2023.

Kuntien tilanne on kirjava. Osalla kaupunkeja on runsaasti resursseja pieniin kuntiin nähden ja siksi tässä lueteltavat keinot ja suositukset kohtaavat ehkä heikommin hyvin pärjäävien kuntien kohdalla.

Selvityksen perusteella operatiivisen tason keskeisin pullonkaula on resurssien puute. Taloudelliset, henkilöstön määrä ja osaaminen toistuvat useimmissa selvityksissä. Digitalisaation katsotaan edistävän palveluiden tarjontaa entistä laajemmille maantieteellisille alueille, mutta se ei poista mm. liitoksiin liittyvää muutoshallinnan vaiheeseen tarvittavia lisäresursseja eikä täydellisesti alueen asukkaiden tarvetta lähipalveluiden tuottamiseen. Integraatioita voitaneen kuitenkin pitää yhtenä suositeltavampana

[22] Valtionhallinnon tehostetun viestinnän ohje – Viestintä normaalioloissa ja häiriötilanteissa (valtioneuvosto.fi) s 17

[23] Kuntaliitokset | Kuntaliitto.fi Kuntarakennelain (1698/2009) tavoitteena on elinvoimainen, alueellisesti eheä ja yhdyskuntarakenteeltaan toimiva kuntarakenne, jolla on taloudelliset ja henkilöstövoimavaroihin perustuvat edellytykset vastata kunnan asukkaiden palvelujen järjestämisestä ja rahoituksesta. Viimeisen 15 vuoden aikana Suomessa on toteutunut 77 kuntaliitosta.

keinona resurssipulan korvaamiseksi, jolloin vähäiset henkilöresurssit ja osaaminen voidaan keskittämällä saada palvelemaan nykyistä laajempaa aluetta.

Operatiivisella tasolla korostunutta resurssivajetta, ulkoisia palveluita ja muutosta kuvataan luvuissa 2.3.1–2.3.3.

Alla olevassa taulukossa on operatiiviselle tasolle suunnattuja

1. esityksiä kehityskohteista,
2. keinoja kehityskohteiden haasteiden minimoimisesta,
3. taustatietoa perusteluissa kehityskohteen haasteesta sekä
4. suosituksia esitettyjen keinojen käyttämisestä.

Kehityskohde	Keino	Perustelu	Suositus
Turvallisuustarkastukset	Auditoinnit ja riippumattomat tarkastukset. Niiden toteuttaminen sekä sopimuksin varmistaminen palveluiden tarjoajilta. Kaikkien turvallisuuden osa-alueiden huomioiminen. Standardien ja muutoin hyväksyttyjen menetelmien laajempi hyödyntäminen.	Organisaation toiminta saattaa olla monitahoista ja siksi kompleksista. Lisäksi ulkopuolinen voi nähdä asiat todellisimpina erilaisten teknisten ja toiminnallisten testien kautta. Osa palveluista on ulkopuolelta hankittua, joten sen laadun takaamiseksi asia on huomioitava palvelusopimuksissa.	Turvallisuustarkastuksissa hyödynnetään alan yrityksiä tai organisaatioita. Perusteena käytetään standardeja, yleisesti hyväksyttyjä menetelmiä (esimerkiksi KATAKRI, JULKRI, PITUKRI) tai teknisiä järjestelmiä. Järjestelmät ja menetelmät testataan teknisesti tai harjoituksissa.
Viestintä	Operatiivisen tason toimijan sisäisen, keskinäisen ja ulkoisen viestinnän parantaminen ja selkeyttäminen normaalioloissa ja häiriötilanteissa. Terminologian yhtenäistäminen. Kyberturvallisuuden tietoisuuden lisääminen. Avoimuuden lisääminen.	Tämän selvitystyön haastatteluvaiheessa nähtiin erittäin tärkeäksi kehittää viestintää erityisesti organisaation sisällä ja sidosryhmissä.	Suunnitellaan ja dokumentoidaan, miten viestintää tulee toteuttaa riittävällä tarkkuudella eri kohderyhmissä (omat työntekijät, sidosryhmät, asiakkaat). Testataan suunnitelma valmentamalla ja harjoituksissa sekä ylläpidetään sitä säännöllisesti. Mukana toiminnan kehittämisessä tulisi olla johto mukana ja sitoutettu.
Osaamisen kehittäminen	Alan oppilaitosten ja työnantajien yhteistyön kehittäminen operatiivisella tasolla ja siten lähennetään opetuksen ja yhteiskunnan tarpeita. Aikuisopetuksen lisääminen verkkokursseilla, tutkinnoilla (oppilaitoksista saatavat pätevyydet sekä sertifikaatit), valmennuksilla ja harjoituksilla.	Oppilaitosten opetus on korkealaatuista, mutta sitä vaivaa opettajapula sekä oppilaitosten ja yhteiskunnan odotusten epätasapaino. Organisaatiot kokevat vastuun omassa henkilöstökoulutuksessa lisääntyneen aiheissa, jotka voitaisiin hoitaa valmistavassa koulutuksessa.	Alaan liittyvää yhteistyötä tulee koordinoida enemmän ja laatia selvityksiä todellisista tarpeista. Operatiivisella tasolla on tunnistettavissa nykyistä enemmän annettavaa muun muassa opetettavien asioiden sisältöihin. Aikuisopetukseen tulisi varata resursseja ja pyrkiä antamaan opetusta ja tutkintoja (ml erilaiset sertifikaatit) eri kielillä.

	Vaatimusten esittäminen valtionhallinnon tai strategisen tason johdon käsiteltäväksi.		Suositellaan sisäisen henkilöstö- ja valmistavan koulutuksen selvittämistä tasapainon löytämiseksi. Organisaatioiden sisäistä koulutusta suositellaan kaikille henkilöstöryhmille.
Toimintaympäristö	Toimintaympäristön analysoinnin lisääminen mm huomioiden arkkitehtuurityö sekä uhkat ja riskit.	Organisaatioiden sisäisen ja ulkoisen toimintaympäristön tunteminen koettiin selvitysten perusteella vaihtelevaksi. Toimintaympäristön tunteminen luo perustan tehokkaalle häiriön- sekä muutosten hallinnalle. Osa uhkista (valtiolliset ihmisperäiset) ovat julkishallinnolle yhteisiä, joten niiden keskitetty seuraaminen ja toiminnasta raportointi parantaisi merkittävästi toimintaympäristön tuntemusta ja riskien hallintaa.	Yksi suositus on lisätä arkkitehtuuriopetusta oppilaitoksissa sekä aloitteleville että jo työelämässä oleville. Lisäksi on suositeltavaa tehdä toimintaympäristön analysointia alaan perehtyneiden asiantuntijoiden avustamana. Analysoinnin tulisi olla jatkuvaa. Valtiollisten toimijoiden arviointi tulisi tehdä keskitetyistä arvioista ja varmistaa tiedonjako operatiivisen tason toimijoille. Lisäksi toimintaympäristöä tulisi katsoa laajemmin kuin vain oman organisaation lähistöltä.
Tilannetietoisuus	Alue- ja paikallistason tilannetietoisuuden tuottaminen. Tilannetiedon saanti strategiselta tasolta sekä palveluiden tarjoajilta. Perusteiden tuottaminen julkisen sektorin toimijoille koskien teknistä valvontaa, tietoa haavoittuvuuksista sekä häiriönhallintaa. ISAC-toiminnan laajentaminen.	Tilannetietoisuus perustuu saatavaan tilannekuvaan. Tilannetietoisuus vaihtelee. Yhtenäistä ja riittävää kuvaa pidetään tavoittelemisen arvoisena.	Riittävän tilannetietoisuuden kehittäminen saattaisi olla mahdollista lisäämällä eri hallinnonalojen välistä yhteistyötä ja selkeyttämällä minkä tasoista tilannekuvaa kukin tuottaa ja mitä voisi muille tarjota sekä itse tarvita. Myös verkostoituminen.
Johtaminen	Pitkän aikavälin johtaminen strategioiden kautta, kehittämällä strategista suunnittelua ja ohjeistusta sekä muutosten hallintaa.	Strategioiden tunteminen, etäisyys ja kattavuus vaihtelevaa.	Johdon sitoutuminen. Arkkitehtuurin kehittäminen. Häiriönhallinnan delegointi.
(Huolto)varmuus	Tietoliikenneyhteyksien ja tietovarantojen kahdennukset, hajauttaminen, segmentointi sekä varautuminen (jatkuvuus- ja valmiussuunnittelu) sekä suunnitelmien testaaminen ovat resilienssin perusta.	Eri selvitysten perustella on jäänyt vaikutelma, että varautumisessa on kehittämisen varaa niin teknisellä kuin toiminnallisella alueella.	Tietovarantojen, tietopalveluiden- tietojärjestelmien- ja tietoliikennearkkitehtuurin laatiminen ja ylläpito. Julkishallinnolle suunnattujen perusteiden hyödyntäminen. Varautumisen suunnittelun toteuttaminen ja ylläpito (harjoittelu). Tarvittaessa ulkoisten asiantuntijoiden hyödyntäminen.

Omatoimisuus	Itsearviointi, testaaminen	Itsearvioinnin työkaluja on kehitetty viime vuosina, mutta niiden hyödyntämistä vaikuttaisi hidastavan resurssipula sekä viestinnän puute (mm. käsitteet) sekä rohkeus testata toimintoja.	Itsearvioitiprosessin kehittäminen avustamalla ensimmäisessä arvioinnissa. Työkalujen ohjeistuksen kehittäminen ja/tai hyödyntäminen esimerkiksi harjoituksissa.
Säädökset	Kehitysohjelmien ja säädösten valmisteluun osallistuminen. Aloitteet.	Yksi julkisen hallinnon suurimmista haasteista on resurssien puute (taloudelliset, henkilöstö ja/tai osaaminen). Säädösten määrän lisääntyminen koettiin syövän jo olemassa olevia resursseja ja kokonaisvaltaisen vaatimusten tason koettiin kasvavan hallitsemattomasti.	Osallistuminen uusien säädösten keskinäisten vaikutusten kokonaisarviointiin jo valmisteluvaiheessa. Resurssitukipyynnöt.
Työkalujen hyödyntäminen	Katakri, julkri, pitukri, standardit, Kybermittari, DVV:n kokonaiskuvapalvelu, arkkitehtuurimalli	Erilaisia työkaluja on kehitetty viime vuosina, mutta niiden hyödyntämistä vaikuttaisi hidastavan resurssipula, viestinnän puute (mm. käsitteet) ja virallisesti hyväksyttyjen arviointiorganisaatioiden vähyys. Teknisen ja toiminnallisen kehityksen myötä osaamisen jatkuva kehittäminen.	Ohjeiden ja standardien päivittäminen. Viestinnän lisääminen. Harjoitusten järjestäminen.
Tukipalvelut	Ohjeet, HelpDesk-toiminta, yhteiset hankkeet	Tietopalveluissa tunnistetaan olevan tukipalveluita, mutta prosessi koettiin hankalaksi ja tuen saanti puutteelliseksi.	Tukipalveluiden käyttäjäystävällisyyden lisääminen sekä tukipalveluiden osaamisen kehittäminen. Palveluvasteen ajan lyhentäminen.
Tekniset toimet	Keskittäminen, segmentointi, varmentaminen	Resurssipula nähtiin ongelmaksi erityisesti pienissä organisaatioissa teknisen ylläpidon osalta.	Keskittämällä voidaan toiminnot hoitaa pienemmillä resursseilla ja oikeilla käyttövaltuustoimilla sekä segmentoinneilla suurten keskittymien turvallisuus voidaan taata riittävällä tasolla.
Verkoston rakenne	Arkkitehtuuri, sopimukset, toimitusketjut, riippuvuudet, omistajuus, kriittiset pisteet, pilvipalvelut	Arkkitehtuurin tilanne oli vaihteleva ja odotukset vaihtelivat oman ja ulkoisen vastuun osalta. Näkymä ulkopuoliseen koettiin heikoksi.	Ulkopuolisten asiantuntijoiden hyödyntäminen. Palvelusopimusten kattavuuden tarkastaminen sekä laadintavaiheessa kattavuuden huomioinen.
Elinkaari	Suunnittelu, toteutus, ylläpito, poistaminen, dokumentaatio	Elinkaaren alkuvaihe aina ylläpitoon vaikuttaa olevan paremmin	Elinkaariosaamisen lisääminen.

		hoidossa kuin poistamiseen liittyvät toimet. Loppuvaiheessa enemmän kehittämistä.	
Varmentaminen	Tietojen varmentaminen tulisi tehdä vähintään kahdentamalla, hajauttamalla, on- ja offline ratkaisuilla. Joissakin tapauksissa paperiset arkistot saattavat edelleen tulla kyseeseen. Varmentamiseen liittyvä toteutus on operatiivisen tason toimia.	3T ympäristöt sisältävät runsaasti arkaluontoista ja esimerkiksi toipumisen kannalta tärkeää tietoa. Eri tapauksissa on käynyt ilmi, että vakavan kyberhyökkäyksen kohteeksi joutunut organisaation on saanut paalutettua toimintansa online-ratkaisuilla, mutta on myös tapauksia, joissa varmennukset ovat saastuneet hyökkäyksen seurauksena käyttökelvottomiksi.	Jokaisen organisaation tulisi tunnistaa, mitä tietoa tarvitaan kyberhyökkäyksestä palautumiseen ja toiminnan jatkamiseen. Tunnistamiseen liittyvä arviointi suositellaan tehtäväksi omien prosessien tai toiminnan tarpeeseen peilaten. Kun edellä mainittu analysointi on tehty, on mahdollista määrittää prosessien ja tietoaineistojen varmentaminen.
Parhaiden käytäntöjen hyödyntäminen	Julkisen materiaalin ”kampaaminen”, oman toimintaympäristön analysoiminen, asiantuntijoiden käyttö (omat tai ulkopuoliset). Käsitteiden ymmärtäminen, käännös työt ja lopputulosten käyttäjäystävällisyys.	Tietovarantojen, tietopalveluiden ja tietojärjestelmien turvaamisen osalta on saatavissa runsaasti informaatiota ja parhaita käytäntöjä. Saatavan tiedon määrä nähdään kuitenkin vaikeaksi löytää ja tunnistaa se sopivaksi omaan toimintaan liittyen.	Taustamateriaalin etsiminen ja sen priorisointi. Apuna voi käyttää oppilaitosten ja alan selvitystöitä tekevien organisaatioiden tutkimusresursseja.

2.3.1 Resurssivaje

Resursseja on kolmenlaisia; taloudelliset, henkilöstön määrä ja henkilöstön osaamistaso. Resurssivaje on todellista eri muotoineen. Esimerkiksi hyvinvointialueiden talous voi olla pahasti alijäämäinen ennen varsinaisen hyvinvointialueen käynnistymistä.[24]

Resurssivajeen korjaamiskeinoja ovat perinteisesti olleet keskittäminen, yhdessä tekeminen ja/tai ulkoistaminen. Se ei ole juuri muuksi muuttunut. Yhtenä mallina on yhden kunnan tai kaupungin nousu keskeiseksi tekijäksi naapurikuntien kanssa. Kaikissa kolmessa vaihtoehdossa on etuna osaamisen keskittäminen ja taloudellisten resurssien pienentäminen. Haittana voidaan kokea etäisyydet sekä operatiivisten että paikallisten tarpeiden ymmärtäminen.

Keskittäminen tai ulkoistaminen ei kokonaan poista operatiivisen tason vaatimusten asettamista. Organisaatioissa, vaikka ovat pieniä, tulee olla riittävä taso organisaation oman toiminnan kannalta tarpeiden määrittelyssä.

[24] Pohjois-Pohjanmaan hyvinvointialue aloittaa yt-neuvottelut henkilöstöjärjestöjen kanssa – ensi vuoden alijäämä voi olla jopa 120 miljoonaa euroa (yle.fi)

2.3.2 Ulkoistetut palvelut

Useimmat operatiivisen tason organisaatioista ovat ulkoistaneet K3TTu:n. Näkymä palveluun voi jäädä siten heikoksi. Näkymää voidaan parantaa palvelusopimusten tai harjoitusten kautta, säännöllisin raportein tai järjestämällä teknisesti pääsy palvelun-tarjoajan digitaaliseen ympäristöön tarkoituksenmukaisessa laajuudessa.

2.3.3 Muutos

Erityisesti sosiaali- ja terveysalalla meneillään oleva muutos on merkittävä. Aikataulu on tiukka ja resurssit puutteelliset tai epäselvät. Useimmat hyvinvointialueet tulevat yh-distämään tietovarantoja, tietopalveluita sekä tietojärjestelmiä. Integroinnin tarve on merkittävä.

Muutoksen hallintakeinoiksi voidaan suositella kattavaa suunnittelua, ulkoista tukea sekä perusteellista arkkitehtuurityötä. Keskeinen asia on myös muutokseen liittyvien riskien tunnistaminen ja hallinta.

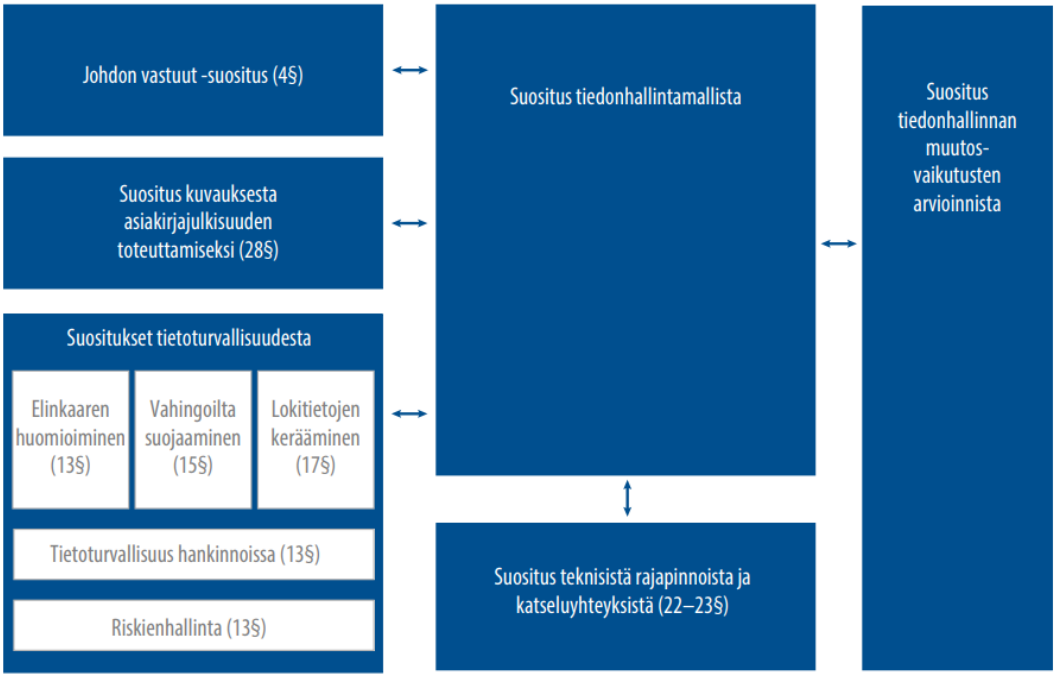
2.4 Lakivelvoitteet

2.4.1 Tietovarantoja, tietopalveluita ja tietojärjestelmiä koskeva lainsäädäntö

Tämän selvityksen kohteena olevia asioita ohjataan eri säädöksin. Niitä ovat tieto-suoja-asetus, julkisuuslaki, tietohallintolaki, arkistolaki ja valmiuslaki.

Esimerkiksi tiedonhallintalaki koskee tietoturvaan liittyviä asioita, sisältäen tietoturvalli-suuteen liittyvät vaatimukset, jotka kaikkien tiedonhallintalain soveltamisalaan sisälty-vien viranomaisten tulee täyttää.[25] Alla olevassa kuvassa on koottu yhteen kuvaus lain eri pykälien sisällyttämästä suosituksesta.

[25] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta : Lautakunnat (valtioneuvosto.fi)



Kuva: Tiedonhallintalakiin liittyvien ensivaiheen tiedonhallinnan suositusten muodostama kokonaisuus[26]

Tiedonhallintalain soveltamisen kannalta 1.1.2023 on keskeinen ajankohta. Se vaikuttaa julkisenhallinnon tilaan ja turvallisuustavoitteisiin.

2.4.2 Tiedonhallinta, tietovarannot ja tietovirrat säädösten näkökulmasta

Tiedonhallintalaki edellyttää tiedonhallintayksikön ylläpitämään sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia. Malli sisältää tiedot mm. toimintaprosesseista, tietovarannoista, tietoaineistoista, arkistoinnista, tietojärjestelmistä ja tietoturvallisuustoimenpiteistä. Se voidaan toteuttaa esimerkiksi kokonaisarkkitehtuurin, tietojärjestelmäarkkitehtuurin, tietovarantokuvausten, asiakirjajulkisuuskuvauksen, tiedonohjaussuunnitelmien ja erilaisten prosessikuvausten avulla. Tiedonhallintayksikkö ylläpitää mallia palvelujen, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi, moninkertaisen tietojen keruun vähentämiseksi, tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteuttamiseksi sekä tietoturvallisuuden ylläpitämiseksi.[27]

Tietoa tulee hallita sen koko sen elinkaaren ajan - tiedon vireille tulosta hävittämiseen tai arkistointiin saakka. Kuvaukset toimivat ja toteuttavat julkisuusperiaatetta sekä toimivat omien tietojen pyyntöön liittyvinä apuvälineinä. Tiedonohjaussuunnitelmilla voidaan todentaa esimerkiksi tietojen säilytysaikojen asianmukainen määrittely, ja että niiden hävittäminen on suunnitelmallista. Tietojen hallinnassa tulee huomioida, että tietovarantoja ja tietojenkäsittelyä hoidetaan myös organisaation ulkopuolella, esimerkiksi useimmissa tapauksissa palkanlaskenta. Organisaatiolla tulisikin olla olemassa

[26] Suositus tiedonhallintamallista (valtioneuvosto.fi) s 12
[27] Tiedonhallintalautakunta: Tiedon elinkaaren vaiheiden hallinta

ohjeistus ja sopimukset näihin ulkoisiin tietojenkäsittelytilanteisiin. Toisaalta organisaatio voi myös käsitellä tietoja käyttäen omia palvelinsalejaan tai ulkoisista pilvipalveluista.[28]

Tietopääoma on organisaation tärkein voimavara, sillä organisaatio voi johtaa tiedolla ja hyödyntää omaa tietopääomaansa vain, jos johdolla on tarpeeksi tietoa muun muassa omasta toiminnasta, toimintaympäristöstään, prosessien toimivuudesta, henkilökunnan osaamisesta, tietovirroista ja tietovarannoista.[29]

3 Yhteenveto

Tämän työn tavoitteena on ollut se, että julkishallinnon toimijoilla olisi keinoja tietovarantojen, tietopalveluiden ja -järjestelmien tunnistamiseen ja niiden saatavuuden ja turvallisuuden varmistamiseen koko elinkaaren ajan (kehitys, tuotanto, tuotannosta poisto).

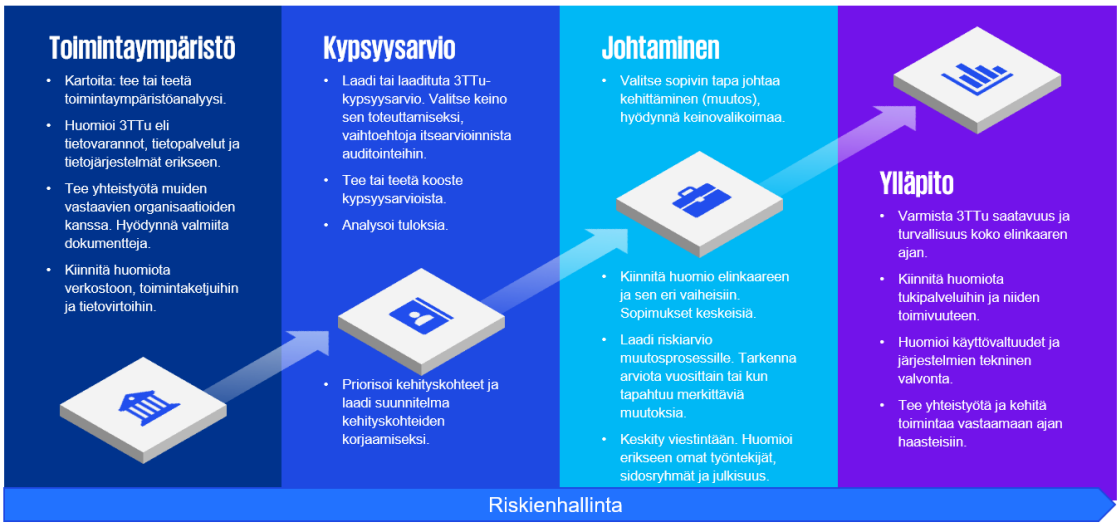
Keinovalikoimia tavoitteeseen pääsemiseksi tunnistettiin useita. Keskeinen kysymys tulee olemaan, miten niitä voidaan parhaiten hyödyntää. Mahdollisuus niiden hyödyntämiseen riippuu muun muassa organisaation roolista, sen henkilöstöstä, ulkoistuksista, resursseista, osaamisesta ja laajuudesta.

Jo selvityksen alkuvaiheessa todettiin, että julkishallinnon kokonaisuuden selvittäminen annetussa ajassa olisi tässä selvityksessä mahdoton tehtävä (mm. yli 300 kuntaa, 21 keskeneräistä hyvinvointialuetta sekä kymmeniä virastoja ja ministeriöitä). Elinkaaren hallinnassa vaikuttaa korostuvan asioiden etupainotteisuus. Kokonaiskuvan tuottaminen on vaativa tehtävä.

Eri selvityksen perusteella voidaan todeta, että tietovarantoja, tietopalveluita ja tietojärjestelmiä on runsaasti. Niiden elinkaarenhallintaa ja turvallisuutta on mahdollista kehittää luetelluilla keinoilla, mutta asioiden pilkkominen pienempiin ja hallittaviin osiin on suotavaa. Useissa asioissa valmentamiseen ja valvontaa liittyviä prosesseja voidaan tuottaa yhteisesti, mutta yksityiskohdat vaihtelevat tapauskohtaisesti.

Edellä mainituista syistä tässä työssä keskityttiin keinovalikoimien esittelyyn. Keinovalikoimien hyödyntäminen riippuu pitkälti siitä, kuinka kehittynyt tietovarantojen, tietopalveluiden ja tietojärjestelmien turvallisuusajattelu ja toteutus koko elinkaaren osalta on kyseessä.

[28] Tiedonhallintalautakunta: Tiedon elinkaaren vaiheiden hallinta
[29] Tiedonhallintalautakunta: Tiedon elinkaaren vaiheiden hallinta



Kuva: Esimerkki keinovalikoiman käytöstä K3TTu työtä tehtäessä

Saatujen havaintojen ja kokemusten perusteella voidaan suositella, että keinojen hyödyntämisessä kannattaa keskittyä avainhenkilöihin ja heidän valmentamiseensa.

Digitaalinen toimintaympäristö olisi hyvä selvittää ja tuntea. Sen hahmottamiseen on useita keinoja, mutta erilaiset arkkitehtuurikuvaukset helpottavat asiaa. Tilannetietoisuuden saamiseksi olisi hyvä arvioida prosessien ja teknisten toimintojen kypsyyttä. Kypsyysarvioiden perusteella voidaan yleensä parhaiten tunnistaa kehityskohteet. Löydökset usein johtavat muutokseen, jonka johtamisessa korostuu kyberturvallisuus. Lisäksi valmiiksi saatu ympäristö vaatii jatkuvaa ylläpitoa, jossa tietoihin liittyvää turvallisuusrakennetta testataan jatkuvasti.

Jatkokehityksen kohteeksi voisi mainita kyberturvallisuuden muutosjohtamisen ohjeen. Sellaista ei ollut tunnistettavissa kotimaisista lähteistä eikä myöskään kansainvälisistä lähteistä.

Toinen jatkoselvityksen ja -kehityksen kohde olisi monihäiriötilannejohtamisen vastuuttaminen, säätely sekä harjoittelu. Keskitetty yhteisten palveluiden tarjoaja voi toimia pikatilanteissa itsenäisesti ja parhaan käsityksensä mukaan, mutta selkeämpi toimintamalli on kehittämisen arvoinen.

Julkishallinnon toimijoilla on useita keinoja tietovarantojen, tietopalveluiden ja -järjestelmien tunnistamiseen ja niiden saatavuuden ja turvallisuuden on varmistamiseen koko elinkaaren ajan (kehitys, tuotanto, tuotannosta poisto). Hyödyntäminen vaatii pitkäjänteistä ja suunnitelmallista työtä, mutta siihen kannattaa panostaa, sillä tieto on arvokkainta omaisuutta, mitä organisaatiolla on olemassa.

Liite 1 Hyödylliset linkit

Digitaalista turvallisuutta käsitteleviä aineistoja on runsaasti saatavilla sekä Suomesta että ulkomailta. Tarjoamme ohessa otoksen käyttöönne. Lähteet ovat julkisia ja niistä kotimaiset on luetteluitu ensimmäisinä. Ulkomaiset viranomaislähteet ovat pääasiassa Euroopan Unionista, ENISASTA, UK:sta ja USA:sta.

Kotimaiset

- Digitaalisen kybermaailman ilmiöitä ja määrittelyjä kybermaailma_v1Fjatk5-0.pdf (jyu.fi)
- Digitaalisen turvallisuuden arkkitehtuuri Digitaalisen turvallisuuden arkkitehtuuri - Digitaalisen turvallisuuden arkkitehtuurin julkinen dokumentaatio - DVV external Confluence
- Digiturvajulkaisut Digiturvajulkaisut | Digi- ja väestötietovirasto | Digi- ja väestötietovirasto (dvv.fi)
- DVV, Digiturvallisuuden hallinta Digiturvallisuuden hallinta (dvv.fi)
- DVV, Oppaat ja hyvät käytännöt Digiturvajulkaisut | Digi- ja väestötietovirasto | Digi- ja väestötietovirasto (dvv.fi)
- eOppiva Digitaalinen turvallisuus järjestykseen arkkitehtuurin avulla - eOppiva
- eOppiva Johdanto kokonaisarkkitehtuuriin - eOppiva
- eOppiva Kokonaisarkkitehtuurin mallintaminen - eOppiva
- eOppiva Turvaa digitaalinen toiminta häiriötilanteissa - eOppiva
- eOppiva TAISTOmaatti - digitaalinen harjoitus organisaation toiminnan ja jatkuvuuden mahdollistamiseksi - eOppiva
- eOppiva Tietosuojan ABC julkishallinnon henkilöstölle - eOppiva
- eOppiva Digiturvallinen työelämä - eOppiva
- eOppiva Riskienhallinta digimaailmassa - eOppiva
- eOppiva Digiturvallisuus hyvinvointialueiden luottamushenkilöille - eOppiva
- eOppiva Digiturvallisuus kuntien luottamushenkilöille - eOppiva
- eOppiva Toimi turvallisesti digimaailmassa - eOppiva
- Julkisen hallinnon strategia Julkisen hallinnon uudistamisen strategia (julkisenhallinnonstrategia.fi)
- Kokonaisarkkitehtuurimenetelmä Kokonaisarkkitehtuurimenetelmä | Suomidigi
- Kuntaliitto, Digitaalinen turvallisuus Digitaalinen turvallisuus | Kuntaliitto.fi
- Kyberturvallisuuden kehittämisohjelma 2021 Kyberturvallisuuden kehittämisohjelma (valtioneuvosto.fi)
- Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus JYX - Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti (jyu.fi)
- Kyberturvallisuuden tilannekuva opetuksesta Tilannekuva kyberturvallisuuden opetuksesta eri koulutusasteilla sekä tarvittavat toimenpiteet määrällisen ja laadullisen kyberturvallisuusosaamistarpeen tyydyttämiseksi saatavilla | FISC

— Kyberturvallisuuskeskus, Kriittisyyden luokittelusta Sote_toimintojen_ja_tietojärjestelmien_kriittisyyden_luokittelu_v1.0.pdf (kyberturvallisuuskeskus.fi)
— Kyberturvallisuuskeskus, Kybermittari Kybermittari | Kyberturvallisuuskeskus
— Kyberturvallisuuskeskus, Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa - ohje johdolle ja asiantuntijoille | Kyberturvallisuuskeskus
— Kyberturvallisuuskeskus, Kyberturvallisuus ja yrityksen hallituksen vastuu Kyberturvallisuus ja yrityksen hallituksen vastuu (kyberturvallisuuskeskus.fi)
— Kyberturvallisuuskeskus, Käytöstä poistuvien palveluiden alasajo Käytöstä poistuvien palveluiden alasajo tulee tehdä huolella | Kyberturvallisuuskeskus
— Kyberturvallisuuskeskus, Näin keräät ja käytät lokitietoja Näin keräät ja käytät lokitietoja | Kyberturvallisuuskeskus
— Kyberturvallisuuskeskus, Näin suojaudut tietomurroilta Näin suojaudut tietomurroilta | Kyberturvallisuuskeskus
— Kyberturvallisuuskeskus, Ohjeita pilvipalveluiden turvallisuudesta Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille | Kyberturvallisuuskeskus
— Kyberturvallisuuskeskus, Pienyritysten kyberturvallisuusopas Pienyritysten kyberturvallisuusopas | Kyberturvallisuuskeskus
— Kyberturvallisuuskeskus, Pitukri Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) (kyberturvallisuuskeskus.fi)
— Kyberturvallisuuskeskus, Toimintaohjeita kyberhyökkäystilanteista toipumiseen Toimintaohjeita kyberhyökkäystilanteista toipumiseen | Kyberturvallisuuskeskus
— Kyberturvallisuuskeskus, Vinkkejä informaatiovaikuttamisen tunnistamiseksi Vinkkejä informaatiovaikuttamisen tunnistamiseksi - Ole tarkkana ja toimi vastuullisesti | Traficom (kyberturvallisuuskeskus.fi)
— KyberVPK Etusivu | KyberVPK
— Sisäministeriö, Alueellisten riskiarvioiden menetelmäohje Alueellisten riskiarvioiden menetelmäohje - Valto (valtioneuvosto.fi)
— Sisäministeriö, Kansallinen riskiarvio 2018 Kansallinen riskiarvio 2018 - Valto (valtioneuvosto.fi)
— Suomen kyberturvallisuusstrategia 2019 Suomen kyberturvallisuusstrategia 2019 – Turvallisuuskomitea
— Suomen kyberturvallisuusstrategia 2013 Suomen kyberturvallisuusstrategia ja taustamuistio-4.pdf (puolustusvoimat.fi)
— THL, määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista THL:n määräys 3/2021 Tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista
— Ulkoministeriö, Katakri Katakri – tietoturvallisuuden auditointityökalu viranomaisille - Ulkoministeriö (um.fi)
— Vahti, Henkilöstön tietoturvaohje VAHTI 4/2013 Henkilöstön tietoturvaohje | Suomidigi

- Vahti, Ohje riskienhallintaan VAHTI 22/2017 Ohje riskienhallintaan | Suomidigi
- Vahti, Tietoturvapoikkeamatilanteiden hallinta VAHTI 8/2017 Tietoturvapoikkeamatilanteiden hallinta | Suomidigi
- Vahti, Toiminnan jatkuvuuden hallinta VAHTI 2/2016 Toiminnan jatkuvuuden hallinta | Suomidigi
- Valtioneuvoston kanslia, Informaatiovaikuttamiseen vastaaminen Informaatiovaikuttamiseen vastaaminen : Opas viestijöille - Valto (valtioneuvosto.fi)
- Valtioneuvoston kanslia, Kyberturvallisuuden strateginen johtaminen Suomessa Kyberturvallisuuden strateginen johtaminen Suomessa - Valto (valtioneuvosto.fi)
- Valtioneuvoston kanslia, Viestintä normaalioloissa ja häiriötilanteissa Valtionhallinnon tehostetun viestinnän ohje : Viestintä normaalioloissa ja häiriötilanteissa - Valto (valtioneuvosto.fi)
- Valtioneuvoston puolustusselonteko Valtioneuvoston puolustusselonteko (ccdcoe.org)
- Valtiovarainministeriö, Julkri Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) : Suositus ja kriteeristö - Valto (valtioneuvosto.fi)
- Valtiovarainministeriö, Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta - Valto (valtioneuvosto.fi)
- Yle uutinen Yle, Tietoturva-alan opiskelijoita ei valmistu riittävästi eikä koulutus vastaa työelämän tarpeita Tietoturva-alan opiskelijoita ei valmistu riittävästi eikä koulutus vastaa työelämän tarpeita, kertoo yliopistotutkimus (yle.fi)
- YTS 2017 Yhteiskunnan turvallisuusstrategia 2017 – Turvallisuuskomitea

Kansainväliset lähteet

- Actions to take when the cyber threat is heightened Actions to take when the cyber threat is heightened - NCSC.GOV.UK ja Actions to take when the cyber threat is heightened (ncsc.gov.uk)
- Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA
- An introduction to computer security: the nist handbook NIST SP 800-12: cover page and Table of Contents (homepage for SP 800-12 in HTML format)
- Asset management Asset management - NCSC.GOV.UK
- ATPs Advanced Persistent Threats (APTs) | Threat Actors & Groups (mandiant.com)
- Bad practices Bad Practices | CISA
- Boosting your organisation’s cyber resilience Boosting your Organisation's Cyber Resilience - Joint Publication — ENISA (europa.eu)
- Building a security operations centre (soc) Building a Security Operations Centre (SOC) - NCSC.GOV.UK
- Building and operating a secure online service Building and operating a secure online service - NCSC.GOV.UK

— Cloud security guidance Cloud security guidance - NCSC.GOV.UK
— Comparative Study on the Cyber Defence of NATO Member States CCDCOE
— Critical Infrastructure sectors Critical Infrastructure Sectors | CISA
— Cyber essentials Cyber Essentials | CISA
— Cyber security culture in organisations Cyber Security Culture in organisations — ENISA (europa.eu)
— Cyber threat map FireEye Cyber Threat Map
— Digital service security Digital Service Security - NCSC.GOV.UK
— Effective steps to cyber exercise creation Effective steps to cyber exercise creation - NCSC.GOV.UK
— NIST, An Introduction to the Components of the Framework An Introduction to the Components of the Framework | NIST
— NIST, Cybersecurity framework Cybersecurity Framework | NIST
— NIST, NISTIR 8286C (riskeistä) NISTIR 8286C, Staging Cybersecurity Risks for ERM and Governance Oversight | CSRC
— NIST, NISTIR 8286 (riskeistä) NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM) | CSRC
— NIST, Risk management framework NIST Risk Management Framework | CSRC
— NIST, SP 800-37 (riskeistä) SP 800-37 Rev. 2, RMF: A System Life Cycle Approach for Security and Privacy | CSRC (nist.gov)
— Mitigating malware and ransomware attacks Mitigating malware and ransomware attacks - NCSC.GOV.UK
— Preparing for the long haul Preparing for the long haul: the cyber threat from Russia - NCSC.GOV.UK
— Protecting bulk personal data Protecting bulk personal data - NCSC.GOV.UK
— Raising awareness of cyber security Raising Awareness of Cybersecurity — ENISA (europa.eu)
— Report on cyber crisis cooperation and management Report on Cyber Crisis Cooperation and Management — ENISA (europa.eu)
— Risk management guidance Risk management guidance - NCSC.GOV.UK
— Risk management standards Risk Management Standards — ENISA (europa.eu)
— Secure communications principles Secure communications principles - NCSC.GOV.UK
— Supply chain security guidance Supply chain security guidance - NCSC.GOV.UK
— Technical Guideline on Minimum Security Measures Technical Guideline on Minimum Security Measures — ENISA (europa.eu)
— Threat landscape for ransomware attacks ENISA Threat Landscape for Ransomware Attacks — ENISA (europa.eu)
— Threat landscape for supply chain attacks Threat Landscape for Supply Chain Attacks — ENISA (europa.eu)
— Top tips for staff Top tips for staff - Overview (ncsc.gov.uk)

— Use of Russian technology products and services Use of Russian technology products and services following... - NCSC.GOV.UK
— Vendor security assessment Vendor Security Assessment - NCSC.GOV.UK
— Zero trust Zero trust architecture design principles - NCSC.GOV.UK
— 10 Steps to Cyber Security 10 Steps to Cyber Security - NCSC.GOV.UK