Kertomusluonnoksesta annetut lausunnot

Sähköisten palveluiden toimintavarmuuden ohjaus (15/2017) 340/54/2015

Valtioneuvoston kanslia, 21.8.2017.
Valtiovarainministeriö, 21.8.2017.
Liikenne- ja viestintäministeriö, 10.8.2017.
Oikeusministeriö, 15.8.2017.
Valtion tieto- ja viestintätekniikkakeskus Valtori, 17.8.2017.
Väestörekisterikeskus, 21.8.2017.
Liikenteen turvallisuusvirasto Trafi, 30.8.2017.
Valtakunnanvoudinvirasto, 17.8.2017.
Oikeusrekisterikeskus, 21.8.2017.

VALTIONEUVOSTON KANSLIA
STATSRÅDETS KANSLI

Lausunto

VNK/1869/01/2016

21.8.2017

Viite: VTV:n lausuntopyyntö Dnro 340/54/2015, 21.6.2017

Valtioneuvoston kanslian lausunto Valtiotalouden tarkastusviraston tuloksellisuus-tarkastuksen "Sähköisten palveluiden toimintavarmuuden ohjaus" tarkastuskertomusluonnoksesta

Valtioneuvoston kansliaa (VNK) on pyydetty tarkastuskertomus-luonnoksen lausuntopyynnössä erityisesti varmistamaan, että kertomukseen ei sisälly asia- tai tulkintavirheitä, joilla olisi vaikutusta tarkastuksen Valtiotalouden tarkastusviraston (VTV) kannanottoihin, sekä kuulla VNK:n näkemys alustavista kannanotoista.

Valtioneuvoston kanslia tuo seuraavassa esille kansliassa tarkastuskertomusluonnoksen käsittelyssä esilletulleita asioita.

Tarkastuskertomus on sisällöllisesti korkeatasoinen vaikka käsittelyn laajuus on asettanut haasteen sen ytimekkyydelle. Tarkastuskertomusluonnoksen sisällysluettelon kuvaannollisista väliotsikoinneista saa kuitenkin nopeasti tiivistelmän kertomuksen päähavainnoista.

Tarkastuskertomuksessa on selkeästi tuotu esiin nykytilanteen haasteet. Lisäksi asiakirjassa on pystytty hyvin tunnistamaan ja kuvaamaan koko valtiotason oleelliset ja keskeisimmät huomattavat havainnot käsiteltävistä asiakokonaisuuksista. Esimerkiksi valtioneuvoston osalta tarkastusluonnoksessa ministeriöiden toiminta-arkkitehtuurien puute ja jatkuvuusriskien hallinnan nykytilanteen kirjavuus oli selkeästi kuvattu. Sama pätee haasteisiin Valtorin palveluiden osalta.

Tarkastuskertomuksen "Johdanto" -kohtaan voisi VNK:n näkemyksen mukaan lisätä vielä huomion, että isoissa organisaatio- ja rakennemuutoksissa ei riitä että vastuut ja budjetti siirretään toimijalta toiselle (transitio). Jotta muutoksella tavoiteltavat edut saavutettaisiin, on aina investoitava sekä

Snellmaninkatu 1, Helsinki | PL 23, 00023 Valtioneuvosto | PUHELIN/TELEFON 0295 16001 (vaihde/växel) | FAKSI/FAX (09) 1602 2165 | kirjaamo@vnk.fi
Snellmansgatan 1, Helsingfors | PB 23, 00023 Statsrådet | | | registratorskontoret@vnk.fi

rahallisesti että toiminnallisesti uuden organisaation toiminnan kehittämiseen (transformaatio). Valtori on tästä hyvä esimerkki: uusia kustannustehokkaita ja parempia palveluita ei ole saatu käyttöön, kun valtaosa organisaatiosta on sidottu vanhojen palveluiden hallinnointiin epäyhtenäisillä ja mahdollisesti kustannustehottomilla tavoilla.

Toinen tarkastuskertomuksen tärkeä havainto on läpinäkyvyyden puute, erityisesti Valtorin toiminnassa. Läpinäkyvyyteen on Valtorin perustamisen yhteydessä luotu huomattavia odotuksia. Ilmiön taustalla on pitkälti Valtorin toiminnan kehittämättömyys sekä osaamiseen liittyvät näkökohdat, jolloin olemassa olevista palveluista ei muodostu palvelun käyttäjille eikä tilaajille kuvaa, ei laadusta eikä aina edes palvelun nykytilanteen sisällöstä tai kehityssuunnista.

Tarkastuskertomuksen "Yhteiset ratkaisut eivät kaikin osin muodosta johdonmukaista kokonaisuutta" –kohdassa on sanottu, että "Valtoria varten perustetun investointimomentin on ajateltu toimivan palvelukehityksen mahdollistajana silloin, kun uudella palvelulla ei olisi vielä riittävästi maksavia asiakkaita". Kuitenkin Valtorilta on kommentoitu myös niin, että tätä momenttia voitaisiin vain käyttää, jotta asiakasvirastot voisivat maksaa Valtorilta tilattuja projekteja ja investointeja takaisin pidemmällä aikavälillä, vaikka Valtorin itsensä kustannukset olisivat jo realisoituneet.

Tarkastuskertomusluonnoksen alussa sivulla 5 oli yhteenvedetty asioita "Tarkastusviraston suositukset" –kohtaan. Valtioneuvoston kanslia on VTV:n kanssa samaa mieltä, että valtiovarainministeriön tulee terävöittää ja muuttaa ohjaustaan entistä konkreettisemmaksi. Jos tämä on kiinni resursseista tai osaamisesta, niin asiat tulee pystyä ratkaisemaan. Tilanne on johtanut siihen, että tosiasialliset päätökset ja linjaukset tehdään edelleen ministeriöissä tai virastoissa itsenäisesti ja toimintalinja on valtiotasolla epäyhtenäinen aiheuttaen lisäkustannuksia ja yhteensopivuuden haasteita.

Vahti-työhön on viimeisten kymmenen vuoden aikana käytetty merkittävästi resursseja, mutta toiminnan vaikuttavuus ei ole nykyisellään riittävä. Syynä voidaan pitää toiminnan painotusta tietoturvan ammattilaisille ja liian yksityiskohtaisia ohjeita. Ohjeiden ja suosituksiin liittyvien kokonaisuuden hallinta on jopa tietoturvallisuuden asiantuntijoille liian haastavaa.

Jatkossa Vahti-ohjeiden ja määräysten valmistelussa ja päivityksissä tulisi nykyistä olennaisesti paremmin pystyä ottamaan huomioon myös toiminnalliset tarpeet etenkin kun toimintaympäristö ja käyttäjien odotukset muuttuvat koko ajan.

Valtioneuvoston kanslia näkee nykytilanteen yhtenä ongelmana erityisesti tietoturvaan liittyen viranomaisten kykyä hallita mitä tietoliikennettä heidän verkoissaan kulkee. Vain muutamalla virastolla tai toimialoilla on tällainen seuranta- ja hallintakyky hankittuna kaupallisilta toimijoilta. Valtori ei kyennyt omassa toiminnassaan saamaan vastaavaa seuranta- ja hallintakykyä ja Valtioneuvoston kanslia pitää tärkeänä kyvykkyyden nopeaa kehittämistä.

Timo Lankinen
Alivaltiosihteeri

Pekka Eerola
Erityisasiantuntija

Valtiontalouden tarkastusvirasto

Viite: VTV:n lausuntopyyntö 21.6.2017 Dnro 340/54/2017

Lausunto tarkastuskertomusluonnoksesta Sähköisten palveluiden toimintavarmuuden ohjaus

Valtiovarainministeriö ilmoittaa pyydettynä lausuntonaan seuraavaa.

Tarkastuskertomusluonnoksessa nostetaan esille niitä seikkoja, joilla voidaan varmistaa ja kehittää julkisen hallinnon sähköisten palvelujen edellyttämää toimintavarmuutta ja oikea-aikaista saatavuutta näiden palveluiden ja organisaatioiden ohjausta kehittämällä. Valtiovarainministeriö huomioi esitetyt suositukset sähköisten palveluiden toimintavarmuuden ohjausta kehittäessä.

Tarkastuskertomusluonnoksessa käsitellään useissa kohdin sisäisen valvonnan ja riskienhallinnan neuvottelukunnassa valmisteltua riskienhallintapolitiikkamallia, josta valtiovarain controller -toiminto on antanut suosituksen. Valtiontalouden tarkastusvirasto esittää tarkastuskertomusluonnoksessaan havaintojaan, tulkintojaan ja kantojaan riskienhallintapolitiikkamallista, sen valmistelusta sekä riskienhallinnan ohjauksen järjestämisestä.

Valtiovarainministeriö esittää tässä lausunnossaan myös valtiovarain controller -toiminnon antamaa taustoittavaa tietoa riskienhallintapolitiikkamallista ja sen valmistelusta, sillä valtiovarain controller -toiminto ei ole ollut tarkastuksen aikana VTV:n haastateltavana tai muuten kuultavana.

Yleisiä huomioita

Tarkastuksen tavoitteet ja tulosten hyödynnettävyys

Tarkastuskertomusluonnoksessa mainitaan tarkastuksen tavoitteeksi tukea hallintoa kehittämään nykyistä ohjausjärjestelmää siten, että ohjausjärjestelmä varmistaa julkisen hallinnon sähköisten palvelujen edellyttämän toimintavarmuuden ja oikea-aikaisen saatavuuden. Liitteen mukaan tarkastuksen tuloksia voidaan hyödyntää tarkastuksen kohteina olevissa organisaatioissa, jotka voivat sen tulosten avulla tunnistaa kehittämiskohteita ja suunnata kehittämistoimia, ja muut organisaatiot saavat tietoa tarkastuksen aikana esiin tulleista hyvistä käytännöistä.

Yleisenä havaintona valtiovarainministeriö esittää, että hyviä käytäntöjä voisi nostaa tekstissä selkeämmin esiin. Myös kehittämissuosituksia voisi selkeyttää ja konkretisoida ylimalkaisia ilmaisuja 'jonkin verran' ja 'kuten esimerkiksi'. Näin tarkastuksen tavoitteet toteutuisivat vielä paremmin ja tarkastuksen tulokset olisivat helpommin hyödynnettävissä hallinnossa.

Taustatietoa

Valtiovarainministeriön osastojen tehtävistä ja työnjaosta

Valtiovarainministeriön tehtävänä on julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Valtiovarainministeriön toimivalta tietoturvallisuuden ja tietohallinnon ohjauksessa ja kehittämisessä perustuu useisiin säädöksiin. Tällaisia ovat laki julkisen hallinnon tietohallinnon ohjaamisesta (634/2011) sekä laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011). Valtiovarainministeriö vastaa turvallisuusverkkotoiminnan yleishallinnollisesta, strategisesta, taloudellisesta ja tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjauksesta ja valvonnasta (10/2015). Valtiovarainministeriön vastuulla on laissa valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä tarkoitettujen yhteisten palvelujen palvelutuotannon yleishallinnollinen, strateginen sekä tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjaus (1226/2013). Valtiovarainministeriön vastuulla on laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016). Nämä tehtävät on valtiovarainministeriössä vastuutettu JulkICT-osastolle.

Valtiovarain controller -toiminnosta säädetään talousarviolaissa (423/1988). Toiminnon yhtenä tehtävänä on mm. ohjata ja sovittaa yhteen sekä kehittää sisäisen valvonnan järjestämistä samoin kuin varmistaa ja edistää valtion talouden ja toiminnan ohjaus- ja raportointijärjestelmien ja -menettelyiden toimivuutta. Valtiovarain controller -toiminnon antamissa sisäisen valvonnan ja riskienhallinnan ohjeissa ja suosituksissa ovat lähtökohtina talousarviolain 24 f §, jossa määritellään toiminnon tehtävät, sekä talousarvioasetuksen (1243/1992) 71 §, jossa on määritelty sisäisen valvonnan ja riskienhallinnan neuvottelukunnan tehtävät.

Valtiovarainministeriöstä annetussa asetuksessa (610/2003) ja valtiovarainministeriön työjärjestyksessä on määritelty tarkemmin ministeriön eri osastojen ohjausvastuut.

Viimeisen kolmen vuoden aikana tapahtuneet hallinnon merkittävät niin ICT-palveluiden organisaatio- kuin hallintamuutokset heijastuvat selkeästi tarkastuskertomusluonnoksen havainnoissa (esimerkiksi Valtorin perustaminen, KaPA-hankekokonaisuus, muut ICT-palvelutuotannossa tapahtuneet muutokset). Valtiovarainministeriö on tunnistanut useimmat sen toimintaan liittyvät havainnot ja kannanotot, joiden osalta kehittämistoimenpiteet ovat etenemässä. Näistä keskeisimmät liittyvät valtiovarainministeriön vastuulla olevien ICT-palveluiden ohjaamisen kehittämiseen sekä uudelleenasetettuun VAHTI-johtoryhmän toimintaan.

Tarkastuskertomuksessa nostetaan riskienhallinnan keskeinen merkitys sähköisten palveluiden koko elinkaarenhallinnan osalta. Valtiovarainministeriö on edistänyt tätä julkaisemalla valtiovarain controller -toiminnon ja sisäisen valvonnan ja riskienhallinnan neuvottelukunnan yhteistyönä riskienhallintapolitiikkamallin sekä tätä tukevan VAHTI-ohjeen, jonka toimeenpanoa toteutetaan osana julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) tuottamaa yhteishanketta yhteistyössä VAHTIn kanssa.

Riskienhallintapolitiikkamallin ja riskienhallinnan ohjeiden valmistelu

Valtiovarain controller -toiminto antoi suosituksen valtionhallinnon riskienhallintapolitiikkamallista 3.5.2017. Riskienhallintapolitiikkamalli ja riskienhallinnan järjestämisen tueksi koottu aineisto on valmisteltu valtioneuvoston asettamassa sisäisen valvonnan riskienhallinnan neuvottelukunnassa, jossa ovat edus-

tettuina kaikki ministeriöt sekä valtiontalouden tarkastusvirasto, Valtiokonttori ja KELA. Neuvottelukunnasta säädetään talousarvioasetuksen (1243/1992) 71 §:ssä ja sen tehtävänä on mm. seurata ja arvioida sisäisen valvonnan ja sen osana olevan riskienhallinnan järjestämisen tilaa ja menettelyitä valtionhallinnossa, tehdä aloitteita sisäisen valvonnan ja sen osana olevan riskienhallinnan kehittämiseksi sekä valmistella ehdotuksia suosituksiksi toimialansa asioissa.

Riskienhallintapolitiikkamallin valmistelussa on lähdetty talousarvioasetuksen (1243/1992) sisäisen valvonnan ja riskienhallinnan järjestämisen vaatimuksesta. Talousarvioasetuksen 69 §:n mukaan viraston ja laitoksen johdon on huolehdittava siitä, että virastossa ja laitoksessa toteutetaan sen talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin riskeihin nähden asianmukaiset menettelyt.

Lähtökohtana on siis ollut viraston oma vastuu ja riskienhallintapolitiikkamalli onkin tarkoitettu virastojen työn tueksi. Neuvottelukunnan tekemän selvityksen mukaan usealla virastolla oli jo riskienhallintapolitiikkoja ja riskienhallinnan käytäntöjä, mutta toisaalta esitettiin toiveita yhteisille välineille ja menettelyille. Riskienhallintapolitiikkamallia valmisteltaessa nähtiin tärkeimmäksi saada aikaan suhteellisen nopeasti riskienhallinnan järjestämiseen virastoja palveleva yksinkertainen malli ja yleisiä ohjeita, joiden perusteella virastot voivat omista tarpeistaan lähtien kehittää riskienhallintaansa. Lisäksi valmistelun keskeisenä lähtökohtana oli näkemys, että riskienhallinta ei ole erillinen toiminto, vaan se tulee ottaa osaksi ohjaus- ja johtamisjärjestelmää, sen tulee kattaa koko toiminta ja toimintamallin on hyvä olla yhtenäinen läpi koko organisaation.

Riskienhallintapolitiikkamalli aineistoineen on valmisteltu pääosin syksyllä 2016. Aineistoluonnoksesta pyydettiin lausuntoja lausuntopalvelu.fi:n kautta 16.12.2016-3.2.2017 ja lausunnoissa esitettyjä parannusehdotuksia otettiin huomioon viimeistelyssä keväällä 2017. Osa lausuntojen ehdotuksista jätettiin vielä jatkokehittämisvaiheisiin.

Päällekkäisen työn välttämiseksi valmistelussa tehtiin tiiviisti yhteistyötä JulkICT:n ja VAHTI-riskienhallintaohjeiden valmisteluryhmän kanssa. Työnjaosta sovittiin siten, että neuvottelukunta valmistelee riskienhallintapolitiikkamallin ja VAHTI-ryhmä käytännönläheisemmät ja syventävät ohjeet. Molempien lausuntokierrokset toteutettiin yhteistyössä suunnilleen samaan aikaan alkuvuonna 2017.

Riskienhallintapolitiikkamalli ja virastojen riskienhallinnan kehittämistä tukeva aineisto julkaistiin suosituksen antamisen yhteydessä nettisivuilla vm.fi/riskienhallinta. Nettitoteutus valittiin, jotta käytännön tueksi tarjotuista aineistoista saadaan helpommin hyödynnettäviä ja ylläpidettäviä. Esimerkiksi riskienhallinnan VAHTI-ohjeiden ilmestyttyä kesäkuussa 2017, ne linkitettiin välittömästi viiteaineistoon.

Huomiot kannanottoihin ja suosituksiin

Näkemyksiä tarkastusviraston kannanottoihin

Tarkastusviraston kannanottona on esitetty: *"Valtiovarainministeriön osastojen, kuten esimerkiksi JulkICT-osaston ja valtiovarain controller-toiminnon, välisessä työnjaossa on jonkin verran päällekkäisyyttä."* (s. 4 pdf-dokumentissa)

Kehittämistä auttaisi, jos VTV voisi vielä täsmentää ja konkretisoida työnjaon päällekkäisyyksiä ja sitä, mihin kannanotto perustuu (säädöspohja, työjärjestykset tms.).

Kannanottoluvun toisella sivulla (pdf-dokumentin s. 5) todetaan seuraavaa: *"Keskitetyt ratkaisut edellyttäisivät myös koko valtionhallinnon käytänteiden yhdenmukaistamista. Valtiovarain controller -toiminto on kehittämässä välineitä yhdenmukaisempaan riskienhallintaan virastotasolla, mutta toimintojen keskittäminen edellyttäisi riskienhallinnan puitteiden luontia myös hallinnonala- ja valtiotasoille."*

Tarkastuskertomusluonnoksen mukaan tarkastusaineiston keruu on päättynyt 2.5.2017. On valitettava yhteensattuma, että tarkastuskertomuksen aineiston hankinta oli rajattu juuri tähän, sillä valtiovarain controller -toiminnon suositus riskienhallintapolitiikkamallista annettiin seuraavana päivänä. Vaikka aineiston keruuaika on rajattava, toivottavasti tarkastuskertomukseen on vielä mahdollista täydentää tieto siitä, että valtiovarain controller -toiminto on 3.5.2017 antanut suosituksen valtionhallinnon riskienhallintapolitiikkamallista sekä koonnut aineistoa hyödynnettäväksi virastojen riskienhallinnan kehittämisessä. Näin kertomuksen lukijalla ei olisi vaarana tulkita VTV:n kannanottoa (erityisesti ilmaisua "on kehittämässä") siten, että on vielä odotettava välineiden valmistumista. Lisäksi perusteena tälle täydennystoiveelle on, että esim. tarkastuskertomusluonnoksessa kuitenkin on jo mainintoja riskienhallintapolitiikkamallin julkaisemisesta.

Myös pdf-sivulle 15 Riskienhallintapolitiikka-laatikkoon olisi tarpeen täydentää vastaava tieto suosituksen antamisesta.

VTV toteaa luonnoksen kannanotoissaan ja havainnoissaan (mm. pdf-sivulla 12), että olisi pitänyt luoda riskienhallinnan puitteet myös hallinnonala- ja valtiotasoille. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnan valmistelu perustui talousarviolainsäädännön lähtökohtiin mm. siitä, että sisäisen valvonnan ja riskienhallinnan järjestäminen on viraston vastuulla. Tavoitteena on ollut virastojen tukeminen, jotta riskienhallintaa ylipäänsä saadaan edistettyä. Riskienhallintapolitiikkamallissa on tarjolla oma kohtansa ministeriön roolista ja vastuusta hallinnonalan riskienhallinnan ohjauksessa.

Valtiontalouden tarkastusvirasto toivoo, että lausunnossa esitetään näkemyksiä tarkastusviraston alustavista kannanotoista. Tarkastuskertomusluonnoksessa on nostettu esille viisi kannanottoa:

Ohjaussuhteita tulee tarkistaa ja ohjeita päivittää vastaamaan nopeasti muuttuvan yhteiskunnan tarpeita

Ohjaustoimet ovat kohdistuneet yksittäisiin virastoihin, mutta tarve ohjata kokonaisuuksia kasvaa jatkuvasti

Toimintavarmuuden turvaamisen kustannuksia, hyötyjä ja toimien riittävyyttä tulee arvioida suhteessa riskeihin

Toimitusketjujen läpinäkyvyydestä tulee huolehtia

Isoissa organisaatio- ja rakennemuutoksissa on turvattava palveluiden toimintavarmuus koko muutosprosessin ajan

Kannanotot ovat hyvin valittuja, valtiovarainministeriö huomioi ne tähän kokonaisuuteen liittyvää ohjausta ja muuta toimintaa kehittäessään, lisätietoa näihin löytyy myöhemmin tästä lausunnosta.

Tarkastusviraston suositukset

Tarkastusluonnoksen viidestä suosituksesta neljä liittyy valtiovarainministeriön toimintaan.

- *valtiovarainministeriö huolehtii siitä, että sen eri osastot ja yksiköt koordinoivat ja sovittavat yhteen ohjaustoimiaan erityisesti riskienhallinnan ohjauksen ja tietohallintoon kohdistuvan ohjauksen osalta*

Kertomuksessa voisi vielä selventää, mitä tämä erityisesti koskee, ts. liittyykö asia nimenomaan kertomusluonnoksen kannanotoissa esitettyyn VTV:n näkemykseen valtiovarain controller -toiminnon ja JulkICT-osaston työnjaon päällekkäisyydestä vai kenties johonkin muuhun ohjaukseen. Valtiovarainministeriön tähän kokonaisuuteen liittyvät tehtävät on kuvattu aikaisemmin lausunnossa. Valtiovarain controller -toiminnon ja JulkICT-osaston yhteistyö on sujuvaa, esimerkiksi riskienhallintapolitiikkamallin ja riskienhallinnan ohjeiden valmistelua on jo koordinoitu ja yhteen sovitettu. Tietohallintoon kohdistuva ohjaus tapahtuu JulkICT-osaston vastuulla, varmistamme ja tarkennamme tätä osana sen ohjauksen kehittämistä.

- *valtiovarainministeriö suunnittelee ja toteuttaa menetelmän, jolla käytännön tueksi tarjotuista ohjekokonaisuuksista, kuten VAHTI, saadaan helpommin hyödynnettäviä, ylläpidettäviä ja toimintaympäristön muutoksiin nopeammin vastaavia*

Valtiovarainministeriö on asettanut uuden julkisen hallinnon digitaalisen turvallisuuden johtoryhmän vuosille 2017-2019, jonka yhtenä tehtävä on toteuttaa uuden tiedonhallintolakikokonaisuuden osana myös tietoturvallisuuden lainsäädäntöä koskeva uudistus. Tätä on jo edistetty siten, että uutta, nykyiset VAHTI-vaatimukset ja ohjeet korvaavaa VAHTI 100-kokonaisuutta on kehitetty vuodesta 2016 alkaen. Tämä kokonaisuus saadaan pilotoitua ja viimeisteltyä vuoden 2018 aikana ennen uuden lainsäädännön suunniteltua voimaan astumista vuonna 2019.

- *valtiovarainministeriö suunnittelee ja ohjeistaa, miten riskienhallinnan puitteet ja käytännöt luodaan hallinnonala- ja valtiotasolle*

Valtiovarain controller ja VAHTI jalkauttavat riskienhallintapolitiikkamallia ja VAHTIn Ohjetta riskienhallintaan, jonka avulla yhdenmukaistetaan tähän liittyviä käytäntöjä. Lisäksi tässä olisi hyvä selventää vielä mm., mihin käyttötarkoitukseen ja kenelle hallinnonala- ja valtiotasoisia riskienhallinnan puitteita ja käytäntöjä tulisi luoda sekä mikä olisi käsittelyfoorumi ja prosessi koko valtionhallinnon tasoiselle riskitarkastelulle.

- *valtiovarainministeriö tarkistaa ja korjaa ohjaustoimiaan Valtorin tilanteen parantamiseksi ja yhdenmukaistaa valtionhallinnon yhteisien tieto- ja viestintäteknisten ratkaisujen ja sähköisten palvelujen tukipalvelujen ohjausta.*

Valtiovarainministeriön JulkICT-osasto on toteuttanut keväällä 2017 sisäisen organisaatiomuutoksen ja tämän lisäksi tämän kokonaisuuden ohjausmallin kehittäminen on käynnissä. Näiden toimenpiteiden tarkoituksena on yhdenmukaistaa JulkICT:n toteuttamaa ohjausta.

Yksityiskohtaiset huomiot

Sivu 13

"Valtiovarainministeriön toimialan määrittely vaikuttaa pääpiirteissään selkeältä, mutta ei kuitenkaan ole täysin selvää, sisältääkö se valtionhallinnon toimijoiden yksityiseltä sektorilta hankkimat palvelut."

Ei sisällä. Jokainen valtionhallinnon toimija vastaa itse omista alihankintasopimuksista ja alihankintaketjuista. Esimerkiksi valtiovarainministeriö ohjaa Väestörekisterikeskusta KaPA-hankkeen / Suomi.fi –palvelukokonaisuuden osalta, mutta väestörekisterikeskus vastaa alihankkijoiden käyttämisestä omilla sopimuksillaan.

Sivu 13

"Valtiovarainministeriön ohjauksessa Kansallinen palveluarkkitehtuuri - ohjelmassa rakennettu kaikille avoin palvelualusta puolestaan palvelee myös yrityksiä pyrkien tarjoamaan alustan uudelle digitaaliselle liiketoiminnalle. Palvelualusta edistää sektorirajat ylittävien sähköisten palvelumarkkinoiden syntymistä osana EU:n sähköisiä sisämarkkinoita. Palvelualustan ohjausvastuut eivät ole valtioneuvoston ohjesäännön perusteella itsestään selviä."

Valtiovarainministeriön ohjauksessa Kansallinen palveluarkkitehtuuri - ohjelmassa on rakennettu yhteentoimiva digitaalisten palvelujen infrastuktuuri, jota myös yritykset voivat lain 571/2016 mukaisesti hyödyntää digitaalisen liiketoiminnan kehittämisessä. Yhteinen infrastruktuuri edistää sektorirajat ylittävien sähköisten palvelumarkkinoiden syntymistä osana EU:n sähköisiä sisämarkkinoita. Valtiovarainministeriö ohjaa sekä KaPa -ohjelman toteuttamista, että ohjelmassa syntyvien Suomi.fi -palveluiden tuottamisesta vastaavaa Väestörekisterikeskusta.

Sivu 13

"Suomen kyberturvallisuusstrategian mukaan kyberturvallisuuden järjestelyissä noudatetaan viranomaisten, yritysten ja järjestöjen välillä vastuunjakoa, joka perustuu säädöksiin ja sovittuun yhteistyöhön. Vaikka toimialajako ei ole kaikin osin selvä, siitä ei ole toistaiseksi aiheutunut suuria ongelmia. Epäselvyydet toimialajaossa voivat kuitenkin aiheuttaa ongelmia jatkossa. On olemassa merkittävä riski siihen, että tehdään päällekkäistä työtä ja annetaan keskenään ristiriitaista ohjausta."

Suomen kyberturvallisuusstrategian toimeenpano-ohjelman v. 2017-2020 toimenpiteinä ovat:

"1) Strateginen johtajuus on määritetty
Liittyy strategiseen linjaukseen: 1,4,5,6,9
Vastuutaho: Turvallisuuskomitean sihteeristö, valtioneuvoston kanslia, valtiovarainministeriö sekä muut tarvittavat toimijat

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

2) Valtionhallinnon kyberturvallisuuden johtamisen malli on luotu ja organisoitu
Vastuutaho: Valtiovarainministeriö
Liittyy strategiseen linjaukseen: 1,2,3

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

Näiden kahden toimeenpano-ohjelmassa olevan toimenpiteen avulla pyritään selventämään tähän kokonaisuuteen liittyvää ohjausta ja vastuunjakoa varmistaen, että tarkastusraportissa esitetty uhka ei toteudu.

Sivu 15

"Pohdintaa siitä, miten voitaisiin tehdä yhteenvetoja riskienhallinnan tilanteesta korkeammalla tasolla, ei kuitenkaan ole tehty.

Lähtökohtana riskienhallintapolitiikkamallissa ja riskienhallinnan järjestämisen ohjeissa on ollut talousarvioasetuksen mukainen viraston vastuu ja nyt on tarjottu välineitä virastojen työn tueksi. Yhteenvedoille olisi mahdollista luoda edellytyksiä esim. riskiluokitteluita yhdenmukaistamalla, mutta lausuntokierroksella monet virastot toivat esiin, että luokitusten tulee olla sovitettavissa virastojen toimintaa parhaiten palvelevaksi. Yhteenvetoja kyllä pohdittiin valmistelun kuluessa. Esillä oli mm. VTV:stä eri yhteyksissä esiin tuotu idea valtiotasoisen riskirekisterin kokoamisesta.

Selkeää toimivaltaa, käsittelyfoorumia ja prosessia koko valtionhallinnon tasoiselle riskitarkastelulle ei kuitenkaan riskienhallintapolitiikkamallin valmistelun kuluessa tunnistettu. Suuritöisiin tiedonkeruisiin ja puitteiden järjestämiseen ei ole tarkoituksenmukaista ryhtyä, ellei ole selvää käsitystä, missä tällaista tietoa hyödynnettäisiin. Hallinnonalatasoisia yhteenvetoja on mahdollista aikaansaada ministeriöiden ohjauksessa, mutta tarpeet näihinkin vaihtelivat. Jos keskitettyjä yhteenvetoja tarvitaan, tulee ensin määritellä, mitä keskitetyt tietotarpeet ovat ja tämän jälkeen voidaan ryhtyä suunnittelemaan tietojen kokoamista.

Sivu 15

"Riskienhallintapolitiikkamallissa on tukeuduttu SFS-ISO 31000 –standardiin. Malli on yleinen. Sen tueksi ei ole tarjottu soveltamisohjeita tai esimerkkejä."

Tarkastuskertomusluonnoksessa kannanotoissaan VTV kritisoi päällekkäistä työnjakoa valtiovarain controller -toiminnon ja JulkICT-osaston välillä. Riskienhallintapolitiikkamallin ja riskienhallinnan ohjeiden valmistelussa nimenomaan pyrittiin välttämään päällekkäistä työtä sillä, että valtiovarain controller -toiminnon työ painottui riskienhallintapolitiikkamallin valmisteluun sisäisen valvonnan ja riskienhallinnan neuvottelukunnassa ja JulkICT-osasto taas keskittyi VAHTI-ryhmässä riskienhallinnan käytännönläheisempien ohjeiden valmisteluun, myös digitaalisen turvallisuuden näkökulmasta. Välittömästi, kun VAHTI-riskienhallintaohjeet oli julkaistu, ne linkitettiin riskienhallintapolitiikkamallin aineistoihin viitemateriaaliin: Ohje riskienhallintaan, Valtiovarainministeriön julkaisuja 22/2017, http://urn.fi/URN:ISBN:978-952-251-862-0

Riskienhallinnan kehittämisen jalkauttamisen edistämiseksi JUHTAn asettama tietoturvan, tietosuojan ja varautumisen asiantuntijaryhmä on käynnistänyt julkisen hallinnon organisaatioille yhteishankkeen, jossa 12.6.2017 – 31.12.2018 toteutetaan 18 työpajaa harjoitustehtävineen,

Sivu 15

"Riskienhallintapolitiikkamallissa ehdotetaan riskien luokittelua perinteisellä tavalla: strategiset, operatiiviset, taloudelliset ja vahinkoriskit. Siitä annetussa esimerkissä tietojärjestelmiin liittyvät riskit luokiteltiin operatiivisiin riskeihin. Annettu esimerkki voi johdattaa tarkastelemaan kyberturvallisuuteen, ICT:hen ja digitalisaatioon liittyviä riskejä liian kapeasti."

Riskienhallintapolitiikkamallissa luokitus on apuväline ja luokitusesimerkkien yhteydessä on mainittu, että virasto voi tarkentaa alajaotteluin tai käyttää muuta, viraston riskienhallintaa paremmin palvelevaa jaottelua. Myös tarkasteltavasta organisaatiosta tai tehtäväalueesta sekä näiden tavoitteista riippuu se, mitkä riskit tunnistetaan strategisiksi.

On ymmärrettävää, että sähköisten palveluiden toimintavarmuuden ohjausta koskevassa tarkastuksessa nousee esiin huoli siitä, että kyberturvallisuuteen, ICT:hen ja digitalisaatioon liittyviä riskejä tarkastellaan liian kapeasti. Vastaava ongelma voisi nousta myös jonkin toisen teeman yhteydessä ja eri näkökulmista asioita tarkastelemalla useimmat riskit voidaan nähdä strategisina riskeinä.

Sivu 15

"Riskienhallinnan taloudellinen näkökulma ei tule riittävästi esille, koska malliin ei sisälly erikseen riskienhallinnasta aiheutuvien kustannusten arviointia. -- Kuitenkin myös riskienhallintapolitiikassa virastoja pitäisi kannustaa miettimään, millä kustannuksilla tulisi pyrkiä pienentämään riskiä tai varautumaan mahdollisiin vahinkoihin. Riskienhallintapolitiikkamalliin sisältyy riskienkäsittelysuunnitelmaksi nimetty liite, jossa voisi olla sarake riskienhallinnan toimenpiteistä aiheutuville kustannuksille ja muille vaikutuksille."

Riskienhallinnan prosessin tiiviissä kuvauksessa on mainittu lyhyesti, että toimenpiteiden tulee olla oikeassa suhteessa riskin kokoon nähden. Jatkokehittämisessä harkitaan VTV:n esittämiä täydennyksiä välineistöön.

Sivu 16

"Mallissa on varsin vähän ehdotuksia siihen, miten riskien tunnistaminen ja arviointi tapahtuvat organisaation eri tasoilla ja miten riskit tarvittaessa tulevat ylimmän johdon käsiteltäviksi. Politiikkamallissa kuvataan riskienhallinnan vastuita ja rooleja. Periaatteessa vastuiden ja roolien kautta voisi olla mahdollista istuttaa riskienhallinta koko organisaatioon ja miettiä, miten ja milloin riskeihin liittyvät tietovirrat eri osapuolten välillä kulkevat."

Riskienhallintapolitiikkamallissa lähestymistapa on se, että riskienhallinta ei ole irrallaan toiminnasta ja organisaatiosta. Mallin tavoitteena on ohjata ja tukea vastuiden ja roolien kautta sekä johtamisjärjestelmään kytkemällä riskienhallinnan istuttamista koko organisaatioon. Mallissa on mm. valmiina kohtia johon virasto voi kirjata esim. työjärjestyksen mukaiset päättävät tahonsa.

Käytännön ohjeita mm. riskien tunnistamiseen ja arviointiin on VAHTI-riskienhallintaohjeessa.

Sivu 16

"Vaikka riskienhallintapolitiikkaa ja VAHTI-ohjetta on pyritty tekemään yhtä aikaa ja koordinoidusti, riskienhallintapolitiikka julkaistiin sen verran aikaisemmin, että sitä ja VAHTI-ohjetta ei välttämättä saatu täysin toisiaan tukevaksi kokonaisuudeksi."

Valtiovarain controller -toiminnon ja sisäisen valvonnan ja riskienhallinnan neuvottelukunnan valmistelun tuloksena syntyi riskienhallintapolitiikkamalli, ei riskienhallintapolitiikka. Tarkoitus on, että mallia voidaan käyttää riskienhallintapolitiikan valmistelun tukena.

Riskienhallintapolitiikkamallin viiteaineistoon päivitettiin linkki VAHTI-ohjeisiin välittömästi sen valmistuttua ja VAHTI-ohjeessa mainitaan, että sisäisen valvonnan ja riskienhallinnan neuvottelukunta on valmistellut valtionhallinnon riskienhallintapolitiikkamallin, josta valtiovarain controller -toiminto on antanut suosituksen 3.5.2017 (http://vm.fi/riskienhallinta).

Kehittämistyötä varten olisi hyvä vielä saada tietää VTV:n käsitys, missä konkreettisesti on vikaa, jotta asiakirjoja saataisiin paremmin toisiaan tukevaksi.

Sivu 16

"On kuitenkin mahdollista, että valtiovarain controller -toiminnon suunnasta tuleva riskienhallinnan ohjaus ei ohjaa virastoja riittävästi tunnistamaan digitalisaatioon liittyviä strategisia riskejä. VAHTI-ohjeet ovat puolestaan leimautuneet tietohallinnosta ja tietoturvasta vastaavien ohjeiksi. Riskienhallinnan ohjaustoimet ovat hajallaan ja kohdistuvat virastoissa eri toimintoihin."

Riskienhallintapolitiikkamalli ja riskienhallinnan järjestämisen tukiaineisto ovat yleisiä. Digitalisaatioon liittyvien strategisten riskien tunnistamiseen liittyvästä ongelmasta on aiemmin tarkastuskertomusluonnoksessa mainittu riskiluokittelun yhteydessä. Riskienhallintapolitiikkamallissa luokitus on kuitenkin vain apuväline ja luokitusesimerkkien yhteydessä on mainittu, että virasto voi tarkentaa alajaotteluin tai käyttää muuta, viraston riskienhallintaa paremmin palvelevaa jaottelua.

Jos riskienhallinta nähdään osana toimintaa, ohjausta tulee pakostakin useammasta lähteestä. Sisäisen valvonnan ja riskienhallinnan neuvottelukunnassa laadittiin perusohjeita ja malleja, joilla tuetaan mm. johtoa organisaation riskienhallinnan järjestämisessä ja ohjauksessa. Yleisten mallien ja ohjeiden lisäksi riskienhallinnan tulisi näkyä osana toimintaa eli eri tehtäväalueilla annettavassa ohjauksessa. Tietohallinnossa ja tietoturvallisuusasioissa riskienhallinta on perinteisesti ollut vahvasti mukana.

Riskienhallinnan ohjeistuksen hajanaisuuden vaikutelman vaara on tunnistettu ja juuri siksi riskienhallintapolitiikkamallin ja VAHTI-ohjeiden valmistelussa tehtiin tiivistä yhteistyötä ja molemmissa aineistoissa ovat keskinäiset viittaukset.

Ohjauksen hajanaisuuteen voisi vielä tulla selkeitä ja konkreettisia korjausehdotuksia VTV:ltä.

Sivu 17

"Toimintamallia, jossa eri hankkeissa kehitettyjä ratkaisuja hyödynnettäisiin vakavissa häiriötilanteissa, ei kehitetty. Valmiuslaki määrittelee karkealla tasolla toimintamallin ja vastuut, mutta kyberturvallisuusstrategiassa ei paneuduttu siihen, miten tunnistetaan laajaksi tai muulla tavoin vakavaksi muuttuva häiriö-

tilanne ajoissa tai miten laajoja häiriötilanteita voisi paremmin ehkäistä etukäteen."

Valtiovarainministeriö tuotti kesällä 2016 päättyneessä SecICT-hankkeessa valtionhallinnon käyttöön useita GovCERT-palveluita, joista yhtenä luotiin VIRT-toimintamalli (Virtual Incident Response Team) laaja-alaisten tieto- ja kyberturvallisuushäiriöiden hallintaan. Toimintamallia on hyödynnetty useassa tällaisessa tilanteessa ja sen kehittämistä jatketaan ja samoin tullaan selvittämään sen laajentamista muualle julkiseen hallintoon.

Tämän ohella osana Suomen kyberturvallisuusstrategian toimeenpanoohjelman v. 2017-2020 toimenpiteenä ovat:

"Julkisen hallinnon kyberhäiriötilanteiden operatiivinen hallintamalli on toteutettu ja toiminnassa
Liittyy strategiseen linjaukseen: 1,2,3,4,5,9
Vastuutaho: Valtiovarainministeriö, liikenne- ja viestintäministeriö, Valtion tieto- ja viestintätekniikkakeskus Valtori"

VIRT-toiminta on liitetty osaksi VAHTI-toimintaa ja valtiovarainministeriö kehittää yhteistyössä muiden vastuutahojen kanssa hallintamallia paremmin vastaamaan muuttuvaa toimintaympäristöä, jossa myös palvelukeskusten rooli huomioidaan paremmin.

Sivu 19

"Uuden tiedonhallintaa koskevan yleislain on tarkoitus tulla voimaan maaliskuussa 2018."

Korjaus: 1.1.2019, asiasta on päätetty Ratkaisujen Suomi: Puolivälin tarkistus, Hallituksen toimintasuunnitelma vuosille 2017–2019.

Sivu 19

"Toimintavarmuuden kannalta keskeinen toiminto on riskienhallinta. Riskienhallinnasta antaa ohjeita ja suosituksia valtiovarain controller -toiminnon lisäksi myös VAHTI."

Valtiovarain controller -toiminnon antamissa ohjeissa ja suosituksissa ovat lähtökohtina talousarviolaki (423/1988) 24 f §, jossa määritellään toiminnon tehtävät, sekä talousarvioasetuksen 71 §, jossa on määritelty sisäisen valvonnan ja riskienhallinnan neuvottelukunnan tehtävät. Riskienhallintapolitiikkamallin valmistelussa lähdettiin talousarvioasetuksen (1243/1992) yleisistä sisäisen valvonnan ja riskienhallinnan järjestämisen vaatimuksesta.

Jos riskienhallinta nähdään osana toimintaa, myös riskienhallinnan ohjeita pitää voida antaa osana toiminnan tai tietyn tehtäväalueen ohjeita. Esim. riskienhallintapolitiikkamallissa ja VAHTI-riskienhallintaohjeissa on pyritty huolehtimaan, että ohjeet eivät ole kohderyhmälle ristiriitaisia.

Sivu 22

"Kyberturvallisuusstrategia on vaikuttanut yksittäisiin virastoihin lähinnä välillisesti. Kyberturvallisuusstrategian kenties näkyvin toimenpide on ollut Kyberturvallisuuskeskuksen perustaminen Viestintäviraston yhteyteen. Muista toi-

mista ovat virastojen kannalta näkyvimpiä Valtorin perustaminen ja hallinnon turvallisuusverkkotoiminnan (TUVE) kehittäminen."

Korjaus: Mikäli muilla toimilla viitataan edelleen Kyberturvallisuusstrategiaan , kohtaa tulee korjata. Valtorin perustaminen ei liity Suomen kyberturvallisuusstrategiaan, vaan se on lähtenyt liikkeelle pääministeri Jyrki Kataisen hallitusohjelmasta 22.6.2011 ("Valtion ICT-palvelukeskusten toimialariippumattomat tehtävät kootaan yhteen."). TUVE-toiminnan kehittäminen on lähtenyt liikkeelle Valtioneuvoston asettamana hankkeena 9.4.2009.

Sivu 24

"VAHTIn ohjeiden rakenne- ja julkaisukanavauudistusta esiteltiin VAHTI-päivässä 13.12.2016. Uudistuksen tavoitteena on ollut myös vähentää vaatimusten lukumäärää. Hankkeen työnimenä on ollut VAHTI 100, millä viitataan vaatimusten tavoitelukumäärään. Hanke eteni aikataulussaan vuoden 2016 aikana, mutta sen jälkeen eteneminen hidastui. Sisältöjen kokoaminen ja muokkaaminen uuden rakenteen mukaisiksi piti tehdä 2016 loppuun mennessä, mutta vielä 13.3.2017 mennessä uudelle sivustolle ei ollut viety yhtään ohjetta. Työn saattaminen päätöksen jäi vuoden 2017 alusta asetetun VAHTI-johtoryhmän tueksi asetettavan asiantuntijajaoston tehtäväksi.

VAHTI-työtä tehdään pääsääntöisesti oman työn ohessa virkatyönä. Uudistustyön työmäärät ovat joko olleet ennakoituja suurempia tai VAHTI-työn uudistaminen on arvioitu muihin virkatehtäviin nähden vähemmän tärkeäksi. "

Johtuen aikaisemmin todetusta tiedonhallintalain voimaantulon aikataulun muuttumisesta maaliskuu 2018 vuoden 2019 alkuun, olemme muuttaneet vastaavasti VAHTI 100-kokonaisuuden aikataulutusta siten, että kokonaisuus saadaan lausunnoille syksyllä 2017. Vaatimusten pilotointi ja viimeistely tehdään vuonna 2018 aikana lainsäädäntötyön viimeistelyn yhteydessä.

Ensimmäinen päivitetty sisältö (VAHTI 100-kortti) julkaistiin sivustolla 24.3.2017. Tuotettua materiaalia on käsitelty kevään ja kesän aikana toteutetuissa VAHTI 100-työpajatilaisuuksissa, joiden perusteella valtiovarainministeriössä on parhaillaan käynnissä vaatimusten ja niihin liittyvien ohjeiden viimeistely.

VAHTI 100-konaisuus on eräs VAHTIn vuosien 2017-2019 kauden ja siihen liittyvän toimeenpano-ohjelman tärkeimpiä kokonaisuuksia (2.1 Tietoturvasäädösten uusiminen ja toimeenpano).

Sivu 25

"Kyselyillä saadaan tilannekatsaus, mutta ei tietoa siitä, mikä on ollut VAHTIn toimenpiteiden vaikutus tilanteeseen tai mitkä syyt selittävät tilannetta. "

Olemme julkaisseet VAHTI-kyselyiden keskeiset tulokset ja niihin liittyvät havainnot ja arvion osana VAHTIn toimintakertomusta. Esimerkiksi VAHTIn vuoden 2015 toimintakertomuksessa sivulla 16 todetaan

"Osa-alueen keskiarvo on laskenut 84 prosentista 79 prosenttiin. Eräs keskeinen syy tähän liittyy useampaan viime vuoden aikana liikkeelle lähteneeseen tai edelleen vaikuttavaan valtionhallinnon ICT-palvelutuotantoon liittyvään muutokseen, esimerkiksi Valtorin käynnistymiseen sekä Valtioneuvoston hallintoyksikön perustamiseen."

Tämä on kuitenkin selkeä havainto, johon tulemme jatkossa kiinnittämään enemmän huomiota. Uudessa vuoden 2017 alussa käynnistyvässä VAHTI-toiminnassa on asetettu erillinen Seurannan ja arviointi –asiantuntijaryhmä kehittämään digitaalisen turvallisuuden seurannan ja mittaroinnin prosesseja, työkaluja ja välineitä.

Sivu 27

"Ohjausmallin mukaisesti valtiovarainministeriön tulisi ohjata Valtoria sen hallituksen kautta tulossopimuksen avulla. Tarkastukseen sisältyneiden haastatteluiden mukaan valtiovarainministeriön ohjaustoimet ovat käyneet lähellä operatiivista johtamista."

Valtiovarainministeriössä on havaittu ohjaustoimien osittainen operatiivisuus Valtorin käynnistymisvaiheessa. Ohjausta on muutettu ohjausmallin mukaiseksi vuoden 2016 aikana, kun Valtorin hallituksen puheenjohtaja sekä toimitusjohtaja vaihtuivat. Valtiovarainministeriö huomioi havainnon käynnissä olevassa ohjausmallin kehittämisessä.

Edellä olevan lisäksi valtiovarainministeriö esittää erillisessä liitteessä teknisluonteisia täsmennysehdotuksia tarkastuskertomusluonnokseen.

Ylijohtaja, ICT-johtaja Anna-Maija Karjalainen

Tietohallintoneuvos, yksikön päällikkö Aku Hilve

Liite 1
Liite valtiovarainministeriön lausuntoon VM/1397/00.05.00/2017 , VTV:n lausuntopyyntö 21.6.2017 Dnro 340/54/2017, Teknisluonteiset huomiot ja korjaukset

Valtiontalouden tarkastusvirasto

Viite: VTV:n lausuntopyyntö 21.6.2017 Dnro 340/54/2017

Liite valtiovarainministeriön lausuntoon VM/1397/00.05.00/2017

Teknisluonteiset huomiot ja korjaukset

Sivu 19

"Uuden tiedonhallintaa koskevan yleislain on tarkoitus tulla voimaan maaliskuussa 2018."

Korjaus: 1.1.2019, asiasta on päätetty Ratkaisujen Suomi: Puolivälin tarkistus, Hallituksen toimintasuunnitelma vuosille 2017–2019.

Sivu 22

"Kyberturvallisuusstrategia on vaikuttanut yksittäisiin virastoihin lähinnä välillisesti. Kyberturvallisuusstrategian kenties näkyvin toimenpide on ollut Kyberturvallisuuskeskuksen perustaminen Viestintäviraston yhteyteen. Muista toimista ovat virastojen kannalta näkyvimpiä Valtorin perustaminen ja hallinnon turvallisuusverkkotoiminnan (TUVE) kehittäminen."

Korjaus: Mikäli muilla toimilla viitataan edelleen Kyberturvallisuusstrategiaan , kohtaa tulee korjata. Valtorin perustaminen ei liity Suomen kyberturvallisuusstrategiaan, vaan se on lähtenyt liikkeelle pääministeri Jyrki Kataisen hallitusohjelmasta 22.6.2011 ("Valtion ICT-palvelukeskusten toimialariippumattomat tehtävät kootaan yhteen."). TUVE-toiminnan kehittäminen on lähtenyt liikkeelle Valtioneuvoston asettamana hankkeena 9.4.2009.

Valtiontalouden tarkastusvirasto
tuloksellisuustarkastus@vtv.fi

Lausuntopyyntö 21.6.2017 340/54/2015

Liikenne- ja viestintäministeriön lausunto sähköisten palveluiden toimintavarmuuden ohjausta käsittelevään tarkastuskertomusluonnokseen

Valtiontalouden tarkastusvirasto on pyytänyt liikenne- ja viestintäministeriön lausuntoa tarkastuskertomusluonnoksesta ”Sähköisten palveluiden toimintavarmuuden ohjaus”.

Tarkastusviraston lausuntopyynnön tarkoituksena on erityisesti varmistaa, että kertomukseen ei sisälly asia- tai tulkintavirheitä, joilla olisi vaikutusta tarkastuksen kannanottoihin, sekä kuulla lausunnonantajien näkemys tarkastusviraston alustavista kannanotoista.

Liikenne- ja viestintäministeriö esittää, että tarkastuskertomusta viimeistelтäessä huomioitaisiin seuraavat havainnot:

Tarkastuskertomusluonnoksessa suositellaan, että liikenne- ja viestintäministeriö varmistaa, että sen käyttämät yhteistyömuodot ja -tavat antavat riittävän lähtökohdan julkista hallintoa koskeville ohjaustoimille. Lisäksi ministeriön tulisi suunnitella ohjaustoimiensa seuranta jatkuvan parantamisen periaatteita noudattaen.

Tarkastuskertomusluonnoksen suositus jää liikenne- ja viestintäministeriön kannalta jossain määrin epäselväksi ja tulkinnanvaraiseksi. Suositus näyttää liittyvän muun muassa tarkastuskertomuksen tietoturvastrategian valmistelusta esitettyihin havaintoihin. Luonnoksessa on esitetty kritiikkiä koskien tietoturvallisuusstrategian suhdetta kyberturvallisuusstrategiaan sekä tietoturvallisuusstrategian valmistelusta kohdassa Suomen tietoturvallisuusstrategian suhde kyberturvallisuusstrategiaan ei ole täysin selvä.

Liikenne- ja viestintäministeriö katsoo, että tarkastuskertomusluonnos antaa varsin puutteellisen kuvan tietoturvallisuusstrategialle asetetuista tavoitteista ja sisällöstä sekä siitä avoimesta valmistelun ja yhteistyön tavasta, jolla liikenne- ja viestintäministeriö on valmistellut ja toimeenpannut tietoturvastrategian hallituksen kärkihankkeiden toimeenpanemisen toimintasuunnitelman tavoitteiden ja lähtökohtien mukaisesti. Kertomusluonnoksessa väitetty epäselvyys tietoturvallisuusstrategian ja kyberturvallisuusstrategian välisessä suhteen näyttää perustuvan siihen, ettei eri strategioiden ja niiden toimeenpano-ohjelmien tehtävänantoja, sisältöä ja sisällöllisiä rajauksia ole huomioitu tarkastuksessa riittävästi. Tarkastuskertomuksessa esitetään myös puutteellisesti tietoturvastrategian toimeenpanon yhteys

Liikenne- ja viestintäministeriö
Käyntiosoite
Eteläesplanadi 16
(kirjaamo)
Helsinki
Postiosoite
PL 31
00023 Valtioneuvosto
Puhelin
029516001
www.lvm.fi
etunimi.sukunimi@lvm.fi
kirjaamo@lvm.fi

tieliikenneturvallisuuden periaatepäätökseen, jonka yhtenä keskeisenä tavoitteena on varmistaa automatisoituvan liikenteen tietoturvallisuus ja liikenneturvallisuus.

Tietoturvallisuusstrategian valmistelu ja toimeenpano perustuvat 28.9.2015 julkistettuun hallituksen toimintasuunnitelmaan strategisen hallitusohjelman kärkihankkeiden ja reformien toimeenpanemisesta, jossa asetettiin strategiatyön keskeiset tavoitteet ja lähtökohdat. Hallituksen toimintasuunnitelman mukaan digitaalisen liiketoiminnan kasvuympäristön rakentamiseen tähtäävän kärkihankkeen osana tulee valtion ja yritysten yhteistyönä laatia tietoturvastrategia, jolla lisätään luottamusta internetiin ja digitaalisiin toimintatapoihin. Hallitus on päivittänyt kärkihankkeiden toimeenpanon toimintasuunnitelman 14.4.2016 ja sisällyttänyt tietoturvallisuusstrategian toteuttamisen edelleen olennaiseksi osaksi digitaalisen liiketoiminnan kasvuympäristön rakentamiseen tähtäävän kärkihankeen toimeenpanoa. Tarkastuskertomusluonnoksessa olisi syytä mainita, että tietoturvallisuusstrategian valmistelu perustui hallitusohjelman kärkihankkeiden toimeenpanosuunnitelmaan, jossa asetettiin strategiatyön keskeiset tavoitteet ja lähtökohdat.

Strategian tulee toimeksiantonsa mukaisesti painottua suomalaisten kilpailukyvyn ja vientiedellytysten varmistamiseen, EU:n digitaalisten sisämarkkinoiden kehittämiseen sekä yksityisyyden suojan ja muiden perusoikeuksien toteutumiseen. Hallituksen toimintasuunnitelman mukaan strategian osana tulee mm. toteuttaa EU:n verkko- ja tietoturvadirektiivin edellyttämät lainsäädäntömuutokset. Hallituksen toimintasuunnitelman mukaan strategialla ja sen toimeenpanolla tulee myös muun muassa lisätä kaupallisten salaus- ja suojausmenetelmien tarjontaa sekä käyttöä. Niin ikään strategian toimeenpanolla tulee parantaa päätelaitteiden, käyttöjärjestelmien, selainten, hakukoneiden, viestintäsovellusten, pilvipalveluiden, ja muiden keskeisten tieto- ja viestintäteknisten hyödykkeiden tietoturvaominaisuuksia sekä kyvykkyyttä havaita ja selvittää tietoturvapoikkeamia. Hallituksen toimintasuunnitelman mukaan valtion roolina tulisi olla luoda luottamusta huolehtimalla lainsäädännön toimivuudesta ja tietoturvaosaamisen kasvattamisesta sekä toimimalla aktiivisesti myös kansainvälisillä foorumeilla.

Tarkastuskertomuksen luonnoksessa todetaan, että tietoturvastrategian valmisteluun osallistui lähinnä vain yrityksiä ja järjestöjä ja etteivät muiden ministeriöiden edustajat olleet mukana strategiatyössä. Luonnoksessa ei kuitenkaan käy ilmi, että tietoturvallisuusstrategian valmistelua tukevassa työryhmässä oli mukana yritysten ja järjestöjen lisäksi myös digitaalisen liiketoiminnan tarjonnan kannalta keskeisinä viranomaisina Viestintävirasto ja Tietosuojavaltuutettu. Lisäksi työryhmä järjesti 15.12.2015 kuulemistilaisuuden, jossa oli kutsuttuna ja edustettuina niin lukuisten ministeriöiden, viranomaisten, yritysten, yliopistojen kuin järjestöjenkin edustajia. Kuulemistilaisuutta seuranneen kirjallisen lausuntokierroksen jälkeen liikenne- ja viestintäministeriö kävi tarkentavia keskusteluja useiden ministeriöiden, muun muassa valtiovarainministeriön, työ- ja elinkeinoministeriön, ulkoasiainministeriön, oikeusministeriön, opetus- ja kulttuuriministeriön, sisäministeriön ja puolustusministeriön kanssa. Strategiasta keskusteltiin myös Valtiovarainministeriön johdolla toimivan laajennetun VAHTI-työryhmän kokouksessa (2.2.2016).

Liikenne- ja viestintäministeriö
Käyntiosoite
Eteläesplanadi 16
(kirjaamo)
Helsinki
Postiosoite
PL 31
00023 Valtioneuvosto
Puhelin
029516001
www.lvm.fi
etunimi.sukunimi@lvm.fi
kirjaamo@lvm.fi

Tietoturvallisuusstrategian valmistelua ja toimeenpanoa on käsitelty kärkihankkeen osana hallituksen strategiaistunnoissa ja toimintatapojen ministeriryhmässä. Kärkihankkeiden etenemistä on käsitelty myös kansliapäällikkökokouksissa. Tietoturvallisuusstrategian etenemistä on kuvattu tiiviisti hallituksen vuosikertomuksissa 2015 ja 2016. Strategian valmistelutilanteesta, toimeenpanosta ja seurannasta on keskusteltu valmistelun ja toimeenpanon aikana säännöllisesti myös digitaalisen liiketoiminnan kasvuympäristön rakentamiseen tähtäävän kärkihankkeen toimeenpanoa koordinoimaan 15.8.2015 asetetussa työryhmässä, jossa edustettuina ovat liikenne- ja viestintäministeriön lisäksi ministeriöistä työ- ja elinkeinoministeriö, valtiovarainministeriö, opetus- ja kulttuuriministeriö sekä sosiaali- ja terveysministeriö.

Liikenne- ja viestintäministeriö teki strategian valmisteluvaiheessa käytyjen keskustelujen pohjalta lukuisia muutoksia työryhmän loppuraporttiin, joka toimi myöhemmin hyväksytyn strategian pohjana. Muille ministeriöille on useissa eri yhteyksissä tarjottu tilaisuus lisätä omaan toimialaansa kuuluvia täydentäviä toimenpiteitä strategiaan. Valmistelun taustat, vaiheet sekä lausuntopalaute on kuvattu avoimesti strategian johdannossa ja perusteluosassa.

Myös strategian toimeenpanossa on tehty hyvin laaja-alaista yhteistyötä eri ministeriöiden, viranomaisten ja yksityisen sektorin yhteisöjen kanssa. Esimerkiksi strategian toimeenpanon kannalta keskeisessä verkko- ja tietoturvadirektiivin kansallisessa täytäntöönpanossa ja täytäntöönpanoa tukemaan 4.10.2016 asetetussa työryhmässä on nimenomaisesti pyritty johdonmukaisesti kuulemaan kaikkia direktiivin soveltamisalan kannalta olennaisia ministeriöitä ja muita viranomaisia. Työryhmässä on ollut edustus direktiivin soveltamisalan kannalta keskeisistä ministeriöitä ja virastoista (työ- ja elinkeinoministeriö, valtiovarainministeriö, sosiaali- ja terveysministeriö, Viestintävirasto, Liikenteen turvallisuusvirasto, Liikennevirasto, Huoltovarmuuskeskus, Finanssivalvonta, Energiavirasto, Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira). Lisäksi työryhmässä on ollut edustus eräistä soveltamisalan kannalta keskeisimmistä yksityisen sektorin yhteisöistä. Työryhmävaiheen jälkeen ministeriö on jatkanut avoimen valmistelutavan mukaisesti keskusteluja soveltamisalan kannalta keskeisten ministeriöiden, virastojen sekä yksityisten yhteisöjen kanssa.

Strategian toimeenpano on säännöllisesti esillä myös VM:n ja LVM:n yhteisissä tapaamisissa, joissa sovitetaan yhteen ministeriöiden toimenpiteitä julkisten palveluiden digitalisointiin ja digitaalisen liiketoiminnan kasvuympäristön rakentamiseen liittyvien kärkihankkeiden toimeenpanossa. Strategian taustasta, valmistelusta ja toimeenpanosta on keskusteltu myös 9.6.2016 hallitusohjelman digitalisaatiotavoitteiden ja julkisen hallinnon ICT-kehittämisen seurantaa varten valtiovarainministeriön 25.12.2015 asettamassa työryhmässä (ns. VM:n DigiNYT-ryhmä).

Myös kyberturvallisuusstrategian toimeenpano-ohjelman päivityksen valmistelun yhteydessä nähtiin, että tietoturvastrategian toimeenpano tuo selkeästi lisäarvoa kyberturvallisuusstrategiaan luotettavan liiketoiminnan ja luotettavien palveluiden edistämisen näkökulmasta. Liikenne- ja viestintä-

Liikenne- ja viestintäministeriö
Käyntiosoite
Eteläesplanadi 16
(kirjaamo)
Helsinki
Postiosoite
PL 31
00023 Valtioneuvosto
Puhelin
029516001
www.lvm.fi
etunimi.sukunimi@lvm.fi
kirjaamo@lvm.fi

ministeriö huomauttaa, ettei tarkastuskertomusluonnoksessa kyberturvallisuusstrategian ja tietoturvastrategian välistä suhdetta arvosteltaessa ole lainkaan huomioitu sitä, että kyberturvallisuusstrategian uuteen toimeenpano-ohjelmaan on yhdeksi toimenpiteeksi kirjattu nimenomaisesti tietoturvallisuusstrategian täytäntöönpano. Tarkastuskertomuksessa asiaa voitaisiinkin selventää toteamalla, että myös kyberturvallisuusstrategian päivitetyssä toimeenpano-ohjelmassa on ristiriidattomasti linjattu toimeenpantavaksi vuoden 2015 ”hallitusohjelman toimeenpanosuunnitelman osana liikenne- ja viestintäministeriön hyväksymä luottamusta internetiin sekä digitaalisiin palveluihin lisäävä tietoturvastrategia”.

Kertomusluonnoksessa myös esitetään, että tietoturvastrategian suhde kyberturvallisuusstrategiaan on esitetty tietoturvallisuusstrategiassa keinotekoisesti. Tietoturvallisuusstrategian perusteluosassa on kuitenkin lausuntopalautteen johdosta erityisesti täsmennetty, että ”strategia on jatkumoa vuosien 2003 ja 2008 tietoturvastrategioille sekä vuoden 2013 kyberturvallisuusstrategialle.” Lisäksi strategian perusteluosassa selvennetään strategioiden suhdetta toteamalla, että ” laadittu strategia painottuu toimeksiantonsa mukaisesti erityisesti digitaaliseen liiketoimintaan sekä tulevasta verkko- ja tietoturvadirektiivistä seuraaviin strategisiin vaatimuksiin.”

Edellä sanotusta johtuen Liikenne- ja viestintäministeriö katsoo, ettei sille tarkastuskertomuksessa esitettyä suositusta tulisi perustaa yksinomaan tietoturvastrategian valmisteluun liittyvään kritiikkiin, joka perustuu osin puutteelliseen tietoon valmistelun taustoista. Lisäksi suosituksessa käytetty ilmaus ”julkista hallintoa koskeville ohjaustoimille” jättää tulkinnanvaraiseksi sen tarkoitetaanko ohjaustoimilla liikenne- ja viestintäministeriön hallinnonalan virastojen ohjausta, koko julkisen hallinnon ohjausta vai ohjaustoimia jotka johtuvat muiden ohjauksesta.

Liikenne- ja viestintäministeriö katsoo, että tarkastuskertomuksessa tulisi selkeämmin avata tietoturvallisuusstrategialle poliittisessa päätöksenteossa määriteltyjä tavoitteita, jotta sen suhde strategiseen hallitusohjelmaan ja muihin poliittisiin strategia-asiakirjoihin avautuisi selkeämpänä. Tarkastuskertomuksessa esitetty kritiikki näyttää perustuvan kolmeen strategian valmisteluvaiheen aikaiseen kirjalliseen lausuntoon, joiden jälkeen mm. strategiatekstiä ja erityisesti strategian tehtävänantoa ja suhdetta kyberturvallisuusstrategiaan on selvennetty niin tietoturvastrategiassa, sen perusteluosassa kuin myös kyberturvallisuusstrategian keväällä 2017 päivitetyssä toimeenpano-ohjelmassa. Kertomuksessa ei ole huomioitu edellä mainittua kärkihankkeiden seurannan ja yhteensovittamisen tarkoituksessa tehtyä yhteistyötä, vaikka tietoturvastrategia on nimenomaisesti osa hallituksen kärkihankkeen toteuttamista. Liikenne- ja viestintäministeriö katsoo, että nämä yhteistyön muodot tulisi avoimesti huomioida kertomuksessa sekä erityisesti arvioitaessa ministeriölle luonnostellun suosituksen tarpeellisuutta.

Tarkastuskertomuksen luonnoksessa todetaan ministeriön pystyneen vain yleisellä tasolla esittämään, miten tietoturvastrategian toimeenpanoa seurataan ja että ministeriön mukaan lopputuloksesta on vaikea sanoa mitään ennen kuin nähdään, minkälaisia tietoaineistoja eri toimijoilla on ja voiko niitä koota yhteen. Liikenne- ja viestintäministeriö huomauttaa, että strate-

Liikenne- ja viestintäministeriö
Käyntiosoite
Eteläesplanadi 16
(kirjaamo)
Helsinki
Postiosoite
PL 31
00023 Valtioneuvosto
Puhelin
029516001
www.lvm.fi
etunimi.sukunimi@lvm.fi
kirjaamo@lvm.fi

gian toimenpiteiden toteutumista seurataan aktiivisesti ja vaikuttavuutta mitataan digitaalisen liiketoiminnan kasvuympäristön rakentamiseen tähtäävälle kärkihankkeelle asetettujen indikaattorien keinoin valtioneuvoston kanslian strategiasihteeristön koordinoimalla tavalla.

Tietoturvallisuusstrategian toteutumisen vaikuttavuutta mitataan mm. selvittämällä edelläkävijäyritysten kasvuodotuksia digitalisaatioon digitaalisen liiketoiminnan kasvuympäristön kärkihankkeen osa-alueilla, joita ovat tietoturvan lisäksi, älykäs liikenne, esineiden internet, massadata sekä robotiikka. Edelläkävijäyritysten kasvuodotuksia tietoturvallisten tuotteiden ja palveluiden sekä muiden kärkihankeen osa-alueilla on selvitetty mm. vuonna 2016 Elinkeinoelämän keskusliiton ja vuonna 2017 Taloustutkimuksen tekemillä haastattelututkimuksilla. Vuoden 2017 tutkimuksen mukaan liikevaihdon ennakoitiin kasvavan jokaisella kärkihankkeen osa-alueella. Investointien ennakoitiin kasvavan robotiikan, tietoturvan ja esineiden internetin alueilla. Vuonna 2017 edellisvuotta useampi vastaaja ennakoi liikevaihdon ja investointien kasvua tietoturvallisten tuotteiden ja palveluiden osa-alueella. Liikenne- ja viestintäministeriö pitäisi perusteltuna, että edellä mainittu huomioitaisiin kertomuksessa tietoturvallisuusstrategian toteutumisen seurantaa ja vaikuttavuutta koskevissa kohdissa.

Tarkastuskertomusluonnoksessa esitetään puutteellisesti myös tietoturvastrategian yhteys tieliikenteen turvallisuuden parantamista koskevaan valtioneuvoston periaatepäätökseen. Liikenne- ja viestintäministeriö toteaa, että tieliikenneturvallisuutta koskevassa 16.12.2016 annetussa valtioneuvoston periaatepäätöksessä – tiedosta liikenneturvallisuutta on linjattu, että automatisoituvan liikenteen turvallisuuden kannalta on tärkeää toteuttaa monien muiden toimien ohella tietoturvallisuusstrategiassa määritellyt toimenpiteet ja valmistella esitys liikennejärjestelmien tietoturvallisuutta parantavan EU:n verkko- ja tietoturvadirektiivin voimaansaattamiseksi. Periaatepäätöksen linjaus korostaa tietoturvallisuuden merkitystä liikenteen automaatiossa sekä huomioi verkko- ja tietoturvadirektiivin yhteyden tieliikenteen älykkään automaation turvallisuuteen. Periaatepäätöksen perusteluosan mukaan tietoturvallisuus tulee huomioida liikennejärjestelmää ja liikennepalveluja suunniteltaessa, kehitettäessä ja ylläpidettäessä. Tämä on tärkeää, jotta tieliikenteen ohjaukseen liittyvät ohjelmistot olisivat laadukkaita ja kestäisivät niin tahallisesti kuin tahattomastikin aiheutuvat tietoturvahäiriöt. On vaikea nähdä perustetta sille, ettei valtioneuvoston periaatepäätöksessä viitattaisi tietoturvastrategian mukaisten toimien toteuttamiseen, kun niillä voidaan edistää automatisoituvan liikenteen turvallisuutta ja tietoturvallisuutta.

Harri Pursiainen
Kansliapäällikkö

Juhapekka Ristola
Osastopäällikkö, ylijohtaja

Liikenne- ja viestintäministeriö
Käyntiosoite
Eteläesplanadi 16
(kirjaamo)
Helsinki
Postiosoite
PL 31
00023 Valtioneuvosto
Puhelin
029516001
www.lvm.fi
etunimi.sukunimi@lvm.fi
kirjaamo@lvm.fi

OIKEUSMINISTERIÖ

LAUSUNTO

OM 8/05/2016
OM 7/05/2016

15.8.2017

tuloksellisuustarkastus@vtv.fi

viite: Lausuntopyyntönne dnro 340/54/2015 ja dnro 185/54/2016

OIKEUSMINISTERIÖN LAUSUNTO TARKASTUSKERTOMUSLUONNOKSIINNE SÄHKÖISTEN PALVELUIDEN TOIMINTAVARMUUDEN OHJAUS JA KYBERSUOJAUKSEN JÄRJESTÄMINEN

Oikeusministeriöllä ei ole kommentoitavaa oikeusministeriötä ja sen hallinnonalan virastoja (Oikeusrekisterikeskus, Valtakunnanvoudinvirasto) koskeviin kohtiin toimintakertomusluonnoksissa.

Pienenä epätarkkuutena Sähköisten palveluiden toimintavarmuuden ohjausta koskevassa tarkastuskertomusluonnoksessa on sivulta 32 löytyvä maininta "Oikeusrekisterikeskus hankkii perustietotekniikkapalvelut Valtorilta", jonka voisi tarkentaa "Oikeusministeriö ja Oikeusrekisterikeskus hankkivat hallinnonalan perustietotekniikkapalvelut Valtorilta". Lisäksi sivulla 34 todetaan "Oikeusrekisterikeskus ja Valtakunnanvoudinvirasto laativat vuosittain toimialasidonnaisten ICT-palvelujen vuosisopimuksen." Tämän lisäksi voisi todeta, että "Oikeusministeriön tietohallintoyksikkö laatii vuosittain palvelusopimuksen Valtorin kanssa hallinnonalan toimialariippumattomien palveluiden tuottamisesta".

Tietohallintojohtaja Tarmo Maunu

Erityisasiantuntija Riitta Marttila

Käyntiosoite	Postiosoite	Puhelin	Faksi	Sähköpostiosoite
Eteläesplanadi 10 HELSINKI	PL 25 00023 VALTIONEUVOSTO	02951 6001	09 1606 7730	oikeusministerio@om.fi

Kommentit VTV:n lausuntopyyntöön tarkastuskertomusluonnoksista Kyberturvallisuuden järjestäminen ja Sähköisten palveluiden toimintavarmuuden ohjaus

Valtorin johtoryhmä ja tuloksellisuustarkastuksiin osallistuneet henkilöt ovat tutustuneet tarkastuskertomusluonnoksiin ja tehneet seuraavassa kuvatut kommentit ja huomiot. Kokonaisuutena Valtori pitää tarkastuskertomusluonnoksia oikeellisina, kattavina ja asianmukaisina.

1 Kybersuojauksen järjestäminen

Luonnoksen mukaan tarkastuksen tavoitteena oli

"*selvittää, onko valtionhallinnon kybersuojaus järjestetty mahdollisimman vaikuttavasti ja taloudellisesti tarkoituksenmukaisella tavalla.*"

Tarkastuskertomuksessa ei arvioida selkeästi asetettujen tavoitteiden toteutumista. Materiaalin perusteella olisi kenties perusteltua sanoa, että tarkastuksen mukaan valtionhallinnon kybersuojauksen vaikuttavuudessa on puutteita, jotka suurelta osin johtuvat kybersuojauksen toteuttamisen puutteellisesta ja epäselvästä rahoituksesta ja resursoinnista.

Tarkastusvirasto ei ehkä riittävän selkeästi kiteytä ja konkretisoi aineistosta selvästi esiin tulevaa kyberturvallisuuden johtamisen liittyvää talouden ongelmaa: ristiriita hyvän tahtotilan ja siihen pääsemisen liittyvien kulujen välillä. Kyberturvallisuuden hoidossa ollaan riippuvaisia rahoitusratkaisuista ja niistä johtuvista resursseista. Valtorin resurssit riippuvat suoraan asiakasvirastojen halusta käyttää ICT-määrärahojaan kyberturvallisuutta kehittävään työhön Valtorissa. Kyberturvallisuuden kehittäminen olisi syytä esittää sellaiseksi, että sen rahoitus ei ole riippuvainen eri asiakasvirastojen panostuksesta ja käytettävissä olevista määrärahoista.

Tarkennetut kommentit luonnoksen sisältöön:

- Kohta 3: ”*Valtori parantaa kybersuojauksen menettelyjen ja kyberloukkausten havainnoinnin toteutusta, arviointia ja kehittämistä*”

Tavoite on ilman muuta oikea, mutta nettobudjetoituna erityisvirastona Valtorin mahdollisuudet toimia rajoittuvat erillisrahoituksen tai palveluiden hinnankorotusten myötä tehtäviin toimenpiteisiin. Tämä on hyvä huomioida myös suosituksissa.

2 Sähköisten palveluiden toimintavarmuuden ohjaus

- Sivu 16: ” Ongelmana on se, että viime kädessä tietoturvallisuudesta vastaa aina varsinaisesta toiminnasta tai palvelusta vastuussa oleva taho.”

Tässä on hyvä tarkentaa, että tietoturvallisuuteen liittyvät vastuut voidaan jakaa kahteen erilliseen kokonaisuuteen: kokonaisvastuu ja toteutusvastuu. Toiminnan, palvelun tai tietojen omistajalla on aina kokonaisvastuu, eli ns. viime käden vastuu tietoturvallisuudesta, mukaan lukien kyseisten kohteiden turvallisuudelta edellytettävän vaatimustason määrittäminen. Tätä vastuuta ei koskaan voida ulkoistaa. Määritettyjen vaatimusten toteutusvastuu voidaan ulkoistaa, kuten tässä tapauksessa Valtorille.

VRK/Pekka Rehn, Ristimäki Pekka

21.8.2017

LAUSUNTO

Viitteet:

Lausuntopyyntö Dnro 185/54/2016 Tarkastuskertomusluonnos Kybersuojauksen järjestäminen
Lausuntopyyntö Dnro 340/54/2015 Tarkastuskertomusluonnos Sähköisten palveluiden toimintavarmuuden ohjaus

VRK/Pekka Rehn, Ristimäki Pekka

21.8.2017

Sisällysluettelo

1 Johdanto 3
2 Kybersuojauksen järjestäminen 3
3 Sähköisten palveluiden toimintavarmuuden ohjaus 4

VRK/Pekka Rehn, Ristimäki Pekka

21.8.2017

LAUSUNTO

1 Johdanto

Väestörekisterikeskus (VRK) kiittää Valtiontalouden tarkastusvirastoa ja sen johtavia tuloksellisuustarkastajia Pirkko Lahdelmaa ja Pasi Korhosta hyvistä havainnoista ja kannanotoista sekä tarkastuksen aikana että tarkastuskertomuksessa. Tarkastus antoi hyvän kuvan kohdealueesta. Erityisen arvokasta oli nostaa osin uusi vaatimus toimia hyvinkin nopeasti verkottuneessa ja nopeasti muuttuvassa toimintaympäristössä ja tuoda selkeästi esiin ettei normaalitilanteessa hyvät toimintatavat pysty välttämättä vastaamaan voimakkaasti integroituneen ympäristön poikkeustilanteiden asettamiin vaatimuksiin.

2 Kybersuojauksen järjestäminen

Sivu 24 (sivun reuna) :

”VRK katsoo Valtorille keskitettyjen tietoturvakontrollien rahoitusongelmien olevan syy VRK:n pirstaloituneeseen kyberturvallisuuden tilannekuvaan”

Täsmennys:

”VRK katsoo Valtorille keskitettyjen tietoturvakontrollien ja Valtorin SSOC:n rahoitusongelmien olevan yksi syy VRK:n pirstaloituneeseen kyberturvallisuuden tilannekuvaan”

Sivu 24:

”VRK:n mukaan Valtori ei ole onnistunut tuottamaan Valtorin palveluiden yhteistä tilannekuvaa asiakasvirastoille ja Kyberturvallisuuskeskukselle. Valtorin tietoturvavalvomon ja Kyberturvallisuuskeskuksen näkyvyys VRK:n palveluihin on huono. VRK:lla pitäisi olla käytössään tietoturvavalvomopalvelu, eikä Valtorin SSOC kata laajasti VRK:n palveluja. VRK:n mukaan valtion tietoturvavalvomotoiminta olisi kuitenkin kustannustehokasta keskittää Valtorin SSOC-toimintoon. VRK katsoo, että jos asiakasmaksuilla tapahtuva rahoitus ei mahdollista laajempaa toimintaa, ratkaisuna voisi olla keskitetty rahoitus.”

Täsmennys:

”VRK:n mukaan Valtori ei ole onnistunut tuottamaan asiakasvirastoille riittävää tilannekuvaa Valtorin palveluiden (TORI) keskeisten kyberturvallisuuteen liittyvien tapahtumien osalta. Valtorin tietoturvavalvomon ja Kyberturvallisuuskeskuksen näkyvyys VRK:n palveluihin (TOSI) ei ole riittävä. VRK:lla pitäisi olla käytössään tietoturvavalvomopalvelu, eikä Valtorin SSOC kata laajasti VRK:n palveluja. VRK:n mukaan valtion tietoturvavalvomotoiminta olisi kuitenkin kustannustehokasta keskittää Valtorin SSOC-toimintoon. VRK katsoo, että jos asiakasmaksuilla tapahtuva rahoitus ei mahdollista laajempaa toimintaa, ratkaisuna voisi olla keskitetty rahoitus.

Valvonta on tehokas toteuttaa keskitetysti mutta keskitetyllä toimijalla ei ymmärrettävästi ole osaamista TOSI-palveluiden valvottavista kohteista ja tapahtumista. Tämä edellyttää yhteistyötä jossa asiakasvirasto yhdessä toteuttajan kanssa määrittelee, luo ja jatkuvasti ylläpitää valvontaa”

VRK/Pekka Rehn, Ristimäki Pekka

21.8.2017

Sivu 36:
"Sertifiointi ei vielä kata KaPA- palveluita..."

Kommentti: KaPa-palveluiden asemesta voi käyttää termiä "Suomi.fi-palvelut" (KaPa-palvelut ovat nykyään Suomi.fi-palveluita).

Sivu 37:

"VRK:lla on käytännön ohjeistusta sovelluskehityksen tietoturvasta, ja tietoturva-asiantuntijat ovat koko ajan mukana kehittämisessä ja konsultoitavissa. Kehityksen lomassa ja vielä ennen käyttöönottoa arvioidaan tietoturvaa ja tietoturva-auditoidaan palveluita. VRK käyttää arviointeihin ulkoisia asiantuntijoita."

Täsmennys:

"VRK:lla on käytännön ohjeistusta sovelluskehityksen tietoturvasta, ja tietoturva-asiantuntijat ovat mukana kehittämisessä ja konsultoitavissa. Tietoturvatestausta tehdään osana ketterää sovelluskehitystä. Ennen sovelluksen/palvelun käyttöönottoa suoritetaan tarpeellisin osin tietoturva-auditointi. VRK käyttää tietoturvatestaukseen ja -auditointeihin ulkoisia asiantuntijoita."

Sivu 40:

"VRK tiedottaa tietoturvaloukkaustilanteessa asiakkaille, osallistuu virka-aikaan häiriön selvitykseen ja tarjoaa sovellustason osaamista käyttöpalvelutoimittajalle. VRK osallistuu VIRT-kokouksiin."

Täsmennys:

"VRK koordinoi tietoturvapoikkeamien selvitystä ja vastaa niistä tiedottamisesta viranomaisille (esim Kyberturvallisuuskeskus) ja asiakkaille sekä muille sidosryhmille poikkeamanhallinta- ja kriisiviestintäohjeistusten mukaisesti. Vakavista tietoturvapoikkeamista ilmoitetaan aina Kyberturvallisuuskeskukselle. VRK osallistuu VIRT-kokouksiin."

3 Sähköisten palveluiden toimintavarmuuden ohjaus

Sivu 5:

"Toiminta-arkkitehtuuri ja strateginen palveluajattelu kehittäisivät toimintavarmuuden suunnittelua ja laajentaisivat näkökulmaa tietohallinnon ulkopuolelle."

Kommentti:

Toiminta-arkkitehtuuri laajentaa näkökulmaa vain, jos tosiallisen toiminta-arkkitehtuuri-työn tekevät tietohallinnon ulkopuoliset henkilöt.

Sivu 36:

"Väestörekisterikeskus otti käyttöönsä vuoden 2016 alussa tietoturvallisuuden tilannekuva- ja toiminnanohjausjärjestelmän Graniten, jolloin myös riskienhallintaprosessi ja -järjestelmä uudistettiin. Graniteen muodostetaan muun muassa riskirekisterit ja hallintajärjestelmät. Tarkastuksen aikana riskienhallintaa ohjasivat Väestörekisterikeskuksen riskienhallintapolitiikka ja riskienhallinnan vuosikello. Riskienhallinnan vuosikello oli välittynyt tietoturvallisuuden hallintajärjestelmän ja yksiköiden tietoturvallisuuden vuosikelloon. Tietoriskejä hallitaan osana viraston kokonaisvaltaista riskienhallintaa. Palvelujen riskienarviointi tehtiin muutamaa lievää poikkeusta lukuun ottamatta riskienhallinnan vuosikellon mukaisesti, mutta

riskienhallinnan toimenpiteitä ei kaikin osin pystytty toteuttamaan aikatauluissaan. Vuoden 2016 aikana oli pyritty vakiinnuttamaan riskienhallinnan käytäntöjä, mutta esimerkiksi tietoturvaryhmän syyskuun kokouksessa havaittiin, että kaikki eivät olleet pitäneet Graniten tietoja riskienhallinnan tehtävistä ajan tasalla. Johdon katselmoinnissa käytiin läpi riskienarvioinnin tuloksia. Tuolloin keskustelua herätti kirjausten taso ja riskien liiallinen määrä. Tunnistettiin tarve keskittyä jatkossa hallintatoimien ja resurssien suuntaamisen näkökulmasta merkittävimpiin riskeihin. Väestörekisteri-keskus itse raportoi riskienhallinnan integroituvan entistä vahvemmin osaksi normaalia liiketoiminnan johtamista."

Kommentti: Granite on tuotenimi, joten ehdotuksena uusi muotoilu.

Uusi muotoilu:

"Väestörekisterikeskus otti käyttöönsä vuoden 2016 alussa tietoturvallisuuden tilannekuva- ja toiminnanohjausjärjestelmän , jolloin myös riskienhallintaprosessi ja -järjestelmä uudistettiin. Järjestelmään muodostetaan muun muassa riskirekisterit, hallitaan vaatimustenmukaisuutta sekä tietoturva- ja auditointipoikkeamia. Tarkastuksen aikana riskienhallintaa ohjasivat Väestörekisterikeskuksen riskienhallintapolitiikka ja riskienhallinnan vuosikello. Riskienhallinnan vuosikello oli välittynyt tietoturvallisuuden hallintajärjestelmän ja yksiköiden tietoturvallisuuden vuosikelloon.Tietoriskejä hallitaan osana viraston kokonaisvaltaista riskienhallintaa. Palvelujen riskienarviointi tehtiin muutamaa lievää poikkeusta lukuun ottamatta riskienhallinnan vuosikellon mukaisesti, mutta riskienhallinnan toimenpiteitä ei kaikin osin pystytty toteuttamaan aikatauluissaan. Vuoden 2016 aikana oli pyritty vakiinnuttamaan riskienhallinnan käytäntöjä, mutta esimerkiksi tietoturvaryhmän syyskuun kokouksessa havaittiin, että kaikki eivät olleet pitäneet tietoja riskien hallintatoimista ajan tasalla.168 Johdon katselmoinnissa käytiin läpi riskienarvioinnin tuloksia. Tuolloin keskustelua herätti kirjausten taso ja aktiivisten riskien liiallinen määrä (hallintatoimet kesken tai jäännösriskiä ei oltu hyväksytty). Tunnistettiin tarve keskittyä jatkossa hallintatoimien ja resurssien suuntaamisen näkökulmasta merkittävimpiin riskeihin. Väestörekisteri-keskus itse raportoi riskienhallinnan integroituvan entistä vahvemmin osaksi normaalia liiketoiminnan johtamista."

Sivu 36:

"Tuolloin keskustelua herätti kirjausten taso ja riskien liiallinen määrä. Tunnistettiin tarve keskittyä jatkossa hallintatoimien ja resurssien suuntaamisen näkökulmasta merkittävimpiin riskeihin. Väestörekisteri-keskus itse raportoi riskienhallinnan integroituvan entistä vahvemmin osaksi normaalia liiketoiminnan johtamista."

Täsmennys:

"Tuolloin keskustelua herätti kirjausten taso ja aktiivisten riskien liiallinen määrä (jäännösriski jäänyt hyväksymättä, tai hallintatoimet kesken). Tunnistettiin tarve keskittyä jatkossa hallintatoimien ja resurssien suuntaamisen näkökulmasta merkittävimpiin riskeihin sekä kiinnittää huomiota riskien yhteismitallisuuteen. Väestörekisterikeskus itse raportoi riskienhallinnan integroituvan entistä vahvemmin osaksi normaalia liiketoiminnan johtamista."

Helsingissä 21.8.2017

Lea Krohns
Ylijohtaja

Pekka Rehn
Johtaja
Esittelijä

Trafi Liikenteen turvallisuusvirasto
Trafiksäkerhetsverket

LAUSUNTO

VTV
tuloksellisuustarkastus@vtv.fi

Päiväys/ Datum 30.08.2017

Dnro/Dnr TRAFI/

Viite/ Referens Lausuntopyyntö 21.6.2017
Dnro 340/54/2015

Lausunto Tarkastuskertomusluonnoksesta Sähköisten palveluiden toimintavarmuuden ohjaus

Valtiontalouden tarkastusvirasto lähettää oheisena luonnoksen tarkastuskertomukseksi ja pyytää antamaan siitä lausunnon. Lausuntopyynnön tarkoituksena on erityisesti varmistaa, että kertomukseen ei sisälly asia- tai tulkintavirheitä, joilla olisi vaikutusta tarkastuksen kannanottoihin, sekä kuulla näkemykset tarkastusviraston alustavista kannanotoista.

Liikenteen turvallisuusvirasto (Trafi) on tarkastellut luonnosta ja esittää seuraavat huomiot.

Tarkastusviraston kannanotot

Tarkastusvirasto suosittaa tarkastuskertomuksessaan seuraavia asioita:

- valtiovarainministeriö huolehtii siitä, että sen eri osastot ja yksiköt koordinoivat ja sovittavat yhteen ohjaustoimiaan erityisesti riskienhallinnan ohjauksen ja tietohallintoon kohdistuvan ohjauksen osalta
- valtiovarainministeriö suunnittelee ja toteuttaa menetelmän, jolla käytännön tueksi tarjotuista ohjekokonaisuuksista, kuten VAHTI, saadaan helpommin hyödynnettäviä, ylläpidettäviä ja toimintaympäristön muutoksiin nopeammin vastaavia
- valtiovarainministeriö suunnittelee ja ohjeistaa, miten riskienhallinnan puitteet ja käytännöt luodaan hallinnonala- ja valtio-tasolle
- valtiovarainministeriö tarkistaa ja korjaa ohjaustoimiaan Valtorin tilanteen parantamiseksi ja yhdenmukaistaa valtionhallinnon yhteisien tieto- ja viestintäteknisten ratkaisujen ja sähköisten palvelujen tukipalvelujen ohjausta.
- liikenne- ja viestintäministeriö varmistaa, että sen käyttämät yhteistyömuodot ja -tavat antavat riittävän lähtökohdan julkista hallintoa koskeville ohjaustoimille. Lisäksi sen tulisi suunnitella ohjaustoimiensa seuranta jatkuvan parantamisen periaatteita noudattaen.

Trafi tukee Tarkastusviraston suosituksia ja näkee erityisen tärkeänä VAHTI-ohjeiden helpomman hyödynnettävyyden sekä Valtorin tilanteen parantamisen.

Tarkastusvirasto kertoo kannanotoissaan valtion omien palvelu-toimittajien, joita ovat esimerkiksi Valtori ja Väestörekisterikeskus, tulee pystyä raportoimaan ja kuvaamaan, miten palveluiden jatkuvuus on turvattu ja kuinka mahdollisista häiriötilanteista toivutaan. Trafin sähköisten palveluiden toimintavarmuus on riippuvainen VRK:n tuottamista suomi.fi-palveluista ja näin ollen Trafi näkee tämän erityisen kriittisenä.

Lisäksi Trafin perustietotekniikan jatkuvuus on riippuvainen Valtorista.

Luku 3.1

Tarkastuskertomuksen luvussa 2.1 tarkastusvirasto kertoo että Trafi on määritellyt järjestelmilleen niiden jatkuvuuteen liittyvät tavoitteet ja tunnistanut kriittiset järjestelmät, mutta ei ole varautunut tilanteeseen, jossa palvelussa oleva vika vaatii paikalle Trafin omaa henkilöstöä virka-ajan ulkopuolella. Trafissa oli tarkastuksen tekohetkellä käynnissä 24/7-selvitys, jonka lopputuloksena Trafin Tietohallinnon tuotantovastaavan päivystys on nyt laajennettu myös virka-ajan ulkopuolelle.

Tarkastuskertomuksen luvussa 2.1 tarkastusvirasto toteaa että Trafin järjestelmien kriittisyyden määrittelyssä ei ole lähdetty kansalaisasiakkaan tarpeista, vaan esimerkiksi ajoneuvorekisterin osalta kriittisyys on ensisijaisesti määritelty varautumisvelvoitteen näkökulmasta. Tämä ei pidä täysin paikkansa; Trafin sähköisissä kansalaispalveluissa kriittisyys on määritelty nimenomaan kansalaisen asiointitarpeen pohjalta ja sen vuoksi kolme kriittisintä ajoneuvojen rekisteröintiin liittyvää palvelua on nostettu 24/7 tasolle. Lisäksi Trafi kerää sähköisistä palveluistaan palautetta säännöllisesti kansalaisilta.

Juhani Nikula
Hallintojohtaja

Heidi Rantanen
Osastopäällikkö

VALTAKUNNANVOUDINVIRASTO

17.8.2017

Lausunto asiassa
VTV Dnro
340/54/2015

Dnro VVV387/331/17

Valtiontalouden tarkastusvirasto
tuloksellisuustarkastus@vtv.fi

Viite Lausuntopyyntö luonnoksesta tarkastuskertomukseksi sähköisten palveluiden toimintavarmuuden ohjauksesta

ASIA Valtakunnanvoudinviraston lausunto

Lausunto Valtakunnanvoudinvirasto lausuu asiassa seuraavaa:

Lausuntopyynnön tarkoituksena on erityisesti varmistaa, että kertomukseen ei sisälly asia- tai tulkintavirheitä, joilla olisi vaikutusta tarkastuksen kannanottoihin, sekä kuulla näkemys tarkastusviraston alustavista kannanotoista.

Valtakunnanvoudinvirasto katsoo, että tarkastuskertomus on asia- ja tulkintasisällöltään oikean sisältöinen, eikä alustavissa kannanotoissa ole huomautettavaa.

Valtakunnanvouti Juhani Toukola

Johtava hallintovouti Veikko Minkkinen

Käyntiosoite	Postiosoite	Puhelin	Telekopio	Sähköpostiosoite
Ratapihantie 9	PL 330	029 56 65180	029 56 65159	vvv@oikeus.fi
00520 HELSINKI	20101 TURKU			

Oikeusrekisterikeskus
PL 157, 13101 HÄMEENLINNA

21.8.2017 Dnro 165/00/2017

Valtiontalouden tarkastusvirasto
Pirkko Lahdelma
PL 1119
00101 HELSINKI

Viite:
VTV/Dnro 340/54/2017

LAUSUNTO TARKASTUSLUONNOKSEEN

Valtiontalouden tarkastusvirasto (VTV) on pyytänyt Oikeusrekisterikeskukselta (ORK) lausuntoa tarkastuskertomusluonnokseen Sähköisten palveluiden toimintavarmuuden ohjauksesta (VTV/Dnro 340/54/2017).

ORK on arvioinut tarkastusluonnoksen ja VTV:n havainnot ja kehittämiskohteet ovat samansuuntaisia kuin mitä olemme itse havainneet. Ei muuta kommentoitavaa.

toimialajohtaja Jari Saarela

kehittämispäällikkö Kimmo Janhunen