Tietoturvallisuus valtioneuvoston kansliassa

Sami Pouttu

2019 Laurea

Laurea-ammattikorkeakoulu

Tietoturvallisuus valtioneuvoston kansliassa

Sami Pouttu
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2019

Laurea-ammattikorkeakoulu
Turvallisuusalan koulutusohjelma

Tiivistelmä

Sami Pouttu

Tietoturvallisuus valtioneuvoston kansliassa

Vuosi 2019 Sivumäärä 38

Valtioneuvoston kansliaa voidaan pitää turvallisuuskriittisenä organisaationa, sillä sen toimintaan ja siellä käsiteltyihin asioihin liittyy sellaisia uhkia, jotka voivat toteutuessaan aiheuttaa huomattavia vahinkoja yleiselle edulle ja turvallisuudelle. Turvallisuuskriittisessä organisaatiossa korostuu kaikkien turvallisuuden osa-alueiden kattava hallinta, sillä kokonaisuus on yhtä vahva kuin sen heikoin lenkki. Opinnäytetyön tavoitteena on muodostaa tilannekuva valtioneuvoston kanslian tietoturvakulttuurin tasosta, tunnistaa mahdolliset heikot lenkit sekä antaa kehitysehdotuksia sen parantamiseksi.

Opinnäytetyö keskittyy tietoturvallisuuden tason mittaamiseen ja kehitysehdotusten luomiseen hallinnollisen tietoturvallisuuden näkökulmasta. Opinnäytetyö rakentuu kolmesta eri vaiheesta, joista kahdessa ensimmäisessä pyritään tutkimaan valtioneuvoston kanslian tietoturvallisuuskulttuuria sekä ymmärtämään sitä ilmiötasolla. Viimeisessä vaiheessa kehitysehdotukset muodostetaan peilaamalla analysoitua tutkimustietoa ja siitä muodostuvaa tilannekuvaa kirjallisuuskatsauksen kautta kerättyyn teoriatietoon.

Opinnäytetyön tuotoksena syntyivät tietoturvallisuuskulttuurin tason tilannekuva sekä siihen pohjautuvat kehittämisehdotukset. Kehitysehdotukset käsitellään kokonaisuudessaan osana opinnäytetyötä. Tilannekuva käsitellään ainoastaan teoria ja menetelmätasolla, mutta varsinainen tuotos rajataan opinnäytetyön ulkopuolelle toimeksiantajan pyynnöstä.

Opinnäytetyön keskeisimpinä havaintoina olivat ohjeiden ja käytänteiden noudattamisen vaikeus sekä puutteet esimiestoiminnassa. Osasyynä havaittuihin poikkeamiin olivat työkäytänteiden ja ohjeistusten välinen ristiriitaisuus, työntekijöiden epäaktiivisuus koulutuksiin osallistumisen suhteen sekä puutteellinen valvonta koulutusten suorittamisen osalta. Opinnäytetyön lopputuotoksena saadut kehitysehdotukset ovat riskitietoisuuden parantaminen, tietoturvakoulutusmallin kehittäminen, esimiestoiminnan tukeminen, kulttuurin kehittäminen sekä tietoturvaohjeiden kehittäminen.

Asiasanat: Tietoturvallisuus, tietoturvallisuusohjeistukset, tilannekuva, turvallisuuskulttuuri

Laurea University of Applied Sciences
Degree Programme in Security Management
Bachelor's Degree

Abstract

Sami Pouttu

Information Security at Prime Minister's Office

Year 2019 Pages 38

The Prime Minister's Office is a security critical organization, because of the threats and risks it is facing in everyday life, which may affect national wellbeing and security. The lifeline of a security critical organization is to take in to account every factor of the security scheme, because the entity of security is as strong as its weakest link. The main objective of this thesis is to develop a model of situational awareness so that the weak links can be identified. A secondary objective of the thesis is to generate development proposals to enhance the current situation.

To develop situational awareness of information security the thesis focuses on measuring the level of information security culture. The thesis also suggest correcting measures from the point of view of information security management. The thesis is carried out in three phases. At the first phase, the thesis focuses on exploring the whole information security culture on organizational level. The second phase investigates deeper causes of the problems that are detected in the first phase with limited group. In the third phase, situational awareness is developed according to points identified from the analyzed information of the two previous phases.

The results of the thesis comprise a situational awareness model and development proposals that aim to the enhancement of the weak spots detected. Situational awareness model is covered in the theoretical section, and the actual model is left out from the thesis at the request of the Prime Minister's Office's representative.

The thesis demonstrates that the main difficulties include following the given policies and deficiencies in the work of supervisors. Some of the reasons for these are the differences between the policies and practice and the lack of contribution in security awareness programs and the lack of supervision of participation. The correcting measures are given in the fifth section and one important point of those is to conduct another survey to control the effects of the correcting measures.
Keywords: Information security, information security policies, security culture, situation awareness

Sisällys

1 Johdanto 6
2 Valtioneuvosto 7
2.1 Valtioneuvoston kanslia 7
2.2 Valtioneuvoston kanslian keskeiset sidosryhmät ja alihankkijat 8
3 Teoreettiset ja käsitteelliset lähtökohdat 9
3.1 Tietoturvallisuus 9
3.2 Organisaatiokulttuuri 9
3.3 Turvallisuuskulttuuri 11
4 Opinnäytetyön toteutusprosessi 12
4.1 Koko organisaatiolle suunnattu kyselytutkimus 13
4.2 Poikkeavalle kohderyhmälle suunnattu haastattelututkimus 19
4.3 Tilannekuvan muodostaminen 22
5 Kehitysehdotukset 24
5.1 Riskitietoisuuden kehittäminen 24
5.2 Koulutusmallin kehittäminen 24
5.3 Kulttuurin kehittäminen 26
5.4 Esimiestoiminnan tukeminen 27
5.5 Ohjeistusten käytettävyyden kehittäminen 28
6 Pohdinta 28
Lähteet 31
Kuviot 34
Liitteet 35

1 Johdanto

Valtioneuvoston kanslian hallintoyksikön tehtäviin kuuluu kehittää valtioneuvoston yhteistä toimintakulttuuria ja valmiusyksikön tehtäviin pitää yllä yleistä tilannekuvaa ja ohjata turvallisuuteen liittyvissä asioissa. Tämän opinnäytetyön tavoitteena on tutkia tietoturvallisuuskulttuurin tasoa valtioneuvoston kansliassa sekä esittää mahdollisia keinoja sen kehittämiseksi tutkimustulosten perusteella.

Opinnäytetyön ensisijainen tavoite on luoda kattava tilannekuva valtioneuvoston kanslian tietoturvallisuuskulttuurin tämän hetkisestä tasosta, sekä toissijaisena tavoitteena luoda kehitysehdotuksia tutkimustulosten perusteella. Opinnäytetyö keskittyy hallinnollisten keinojen kehittämiseen tietoturvallisuuskulttuurin näkökulmasta. Hallinnollisten ja teknisten keinojen rajapinta on häilyvä, joten myös teknisiä tekijöitä sivutaan opinnäytetyön eri vaiheissa, mutta varsinaiset kehittämiseen liittyvät työvaiheet rajataan koskemaan vain hallinnollisia ratkaisuja.

Alihankkijoiden ja palveluntoimittajien keskeisestä asemasta huolimatta tämän opinnäytetyön tutkimukset toteutettiin ainoastaan valtioneuvoston kanslian työntekijöille. Opinnäytetyön kehitysehdotuksissa otetaan kuitenkin huomioon alihankkijoiden ja palveluntoimittajien vastuut, sekä mahdolliset kehitysehdotukset niiden osalta.

Opinnäytetyö kohdistuu suhteellisen arkaluonteiseen asiakokonaisuuteen ihmisten yksityisyyden ja työtapojen analysoinnin vuoksi. Tämän vuoksi yksityisyydensuojan ja anonymiteetin säilymiseen ja siitä viestimiseen panostettiin koko opinnäytetyöprosessin ajan. Ensimmäinen tutkimus suoritettiin täysin anonyymisti, eikä työntekijöitä ole mahdollista yksilöidä tutkimustuloksista. Toinen tutkimusvaihe suoritettiin luottamuksellisesti, eikä työpajoissa ilmenneitä poikkeamia tai yksityiskohtia ilmaista tutkimuksen tuloksissa niin että osallistujat olisivat pääteltävissä tuotoksesta.

Tutkimus pyrittiin toteuttamaan hyvien tutkimustapojen mukaan ja kaikki työvaiheet kirjaamaan mahdollisimman tarkasti toistettavuuden varmistamiseksi. Valtioneuvoston kanslia on kuitenkin ympäristönä ainutlaatuinen ja tämän vuoksi kaikki tutkimuksessa käytetyt menetelmät eivät välttämättä sovellus toteutettavaksi normaalissa työympäristössä.

Opinnäytetyön eri vaiheissa on tärkeää saada ulkopuolisten näkemyksiä tekstistä, jotta opinnäytetyö pysyy annettujen raamien sisällä, sekä että valitut näkökulmat ja metodit tukevat annettujen tutkimuskysymysten selvittämistä (Hirsjärvi, Remes, & Sajavaara 1997, 49). Tämän varmistamiseksi opinnäytetyön tuloksista ja etenemisestä viestittiin jokaisen työvaiheen välissä oppilaitoksen edustaman opinnäytetyön ohjaajan kanssa. Opinnäytetyön tilaajan (VNK) edustajan kanssa tietojenvaihto sidottiin osaksi arkipäiväistä työrutiinia harjoittelun sen mah-

dollistaessa. Opinnäytetyön eri vaiheista keskusteltiin viikoittaisella tasolla ja kaikki tutkimuksissa havaitut tulokset käytiin läpi ennen seuraavan työvaiheen aloittamista. Mikäli alkuperäinen suunnitelma vaati muutoksia, hyväksytettiin ne ensin opinnäytetyötä ohjaavan VNK:n edustajan kanssa.

Opinnäytetyö tehtiin julkisena, mutta organisaation toimintaympäristön ja käsiteltävien aineistojen vuoksi joitain tutkimuksen taikka tuotosten osioiden käyttöä jouduttiin rajoittamaan opinnäytetyön ulkopuolelle. Ensimmäisen ja toisen vaiheen tutkimukset käsitellään opinnäytetyössä menetelmätasolla, jota täydennetään muutamilla tutkimusaineiston havainnoilla suoritetun tutkimusprosessin selkeyttämiseksi. Toisen vaiheen tutkimuksen tulosten tarkempi käsittely jätetään pois opinnäyteyöstä, sillä ne ovat keskeinen osa muodostettavaa tilannekuvaa, jota ei julkaista toimeksiantajan pyynnöstä. Tilannekuva käsitellään ainoastaan teoriatasolla opinnäytetyön julkisessa osassa. Opinnäytetyön toinen tavoite, eli kehitysehdotukset käsitellään julkisena osana opinnäytetyötä.

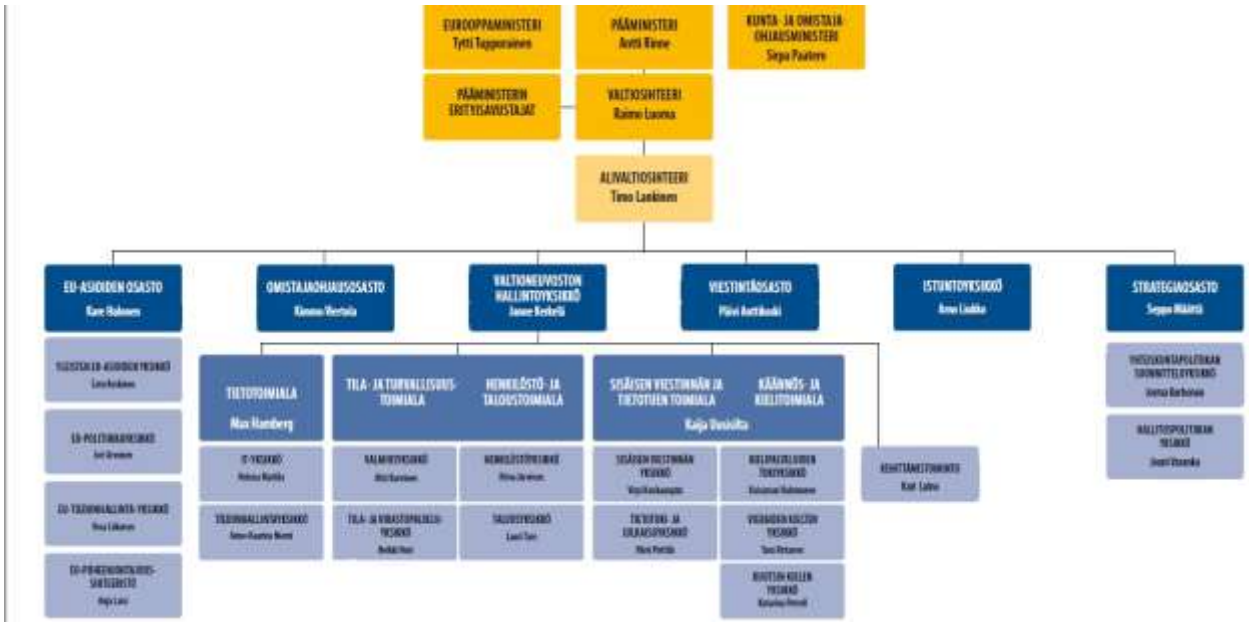
2 Valtioneuvosto

Valtioneuvoston verkkosivujen mukaan valtioneuvostolla voidaan tarkoittaa joko pääministeristä ja ministereistä koostuvaa yleistä hallintovaltaa käyttävää toimielintä taikka valtioneuvoston yleisistunnon ja ministeriöiden muodostamaa päätöksentekoelintä (Valtioneuvosto). Tässä opinnäytetyössä valtioneuvostoa tarkastellaan ministeriöiden näkökulmasta ja se on rajattu koskemaan ainoastaan valtioneuvoston kanslian henkilökuntaa.

2.1 Valtioneuvoston kanslia

Valtioneuvoston kanslia on pääministerin johtama ministeriö, joka vastaa hallitusohjelman toimeenpanon valvonnasta ja avustaa pääministeriä valtioneuvoston johtamisessa. Ministeriön tehtäviin kuuluvat mm. Suomen EU-politiikan yhteensovittaminen, valtioneuvoston kanslian alaisten valtion yhtiöiden omistajaohjaus, valtioneuvoston viestinnän ohjaus ja yhteensovittaminen, tilannekuvan järjestäminen, varautuminen ja turvallisuus, häiriötilanteisen yhteensovittaminen sekä pääministerin ja hallituksen toimintaedellytysten varmistaminen kaikissa tilanteissa (Valtioneuvosto).

Pääministerin lisäksi valtioneuvoston alaisuudessa toimivat elinkeinoministeri, kunta- ja uudistusministeri sekä Eurooppa-, kulttuuri- ja urheiluministeri. Toiminnan johtamisessa pääministeriä avustavat valtiosihteeri sekä alivaltiosihteeri. Valtioneuvoston organisaatio koostuu viidestä yksiköstä, jotka ovat EU-asioiden osasto, omistajaohjausosasto, valtioneuvoston hallintoyksikkö, viestintäosasto sekä strategia osasto. Lisäksi valtioneuvoston alaisuuteen kuuluvat kehittämistoiminto, hallituspolitiikan yksikkö, yhteiskuntapolitiikansuunnitteluyksikkö sekä istuntoyksikkö. Koko valtioneuvoston kanslian organisaatio on nähtävissä kuviosta 1.



Kuvio 1: Valtioneuvoston kanslian organisaatio (valtioneuvoston kanslia)

Valtioneuvoston kanslian valmiusyksikkö on valtioneuvoston kanslian hallintoyksikön tila- ja turvallisuustoimialan alainen yksikkö, jonka yhtenä tehtävänä on valtioneuvoston ja sen ministeriöiden yhteisen turvallisuuden ja tietoturvallisuuden ohjaus ja yhteensovittaminen

2.2 Valtioneuvoston kanslian keskeiset sidosryhmät ja alihankkijat

Valtori, eli valtion tieto- ja viestintätekniikkakeskus on valtiovarainministeriön ohjaama virasto, jonka tehtävänä on tuottaa kaikki perus ICT-palvelut valtionhallinnon virastoihin ja laitoksiin (valtori). Valtori vastaa ICT-palveluiden tuotannosta koko valtioneuvostolle ja valtioneuvoston kanslia, yhdessä valtiovarainministeriön kanssa, palvelun tuotannon tason valvomisesta.

Senaatti-kiinteistöt vastaa valtionhallinnon kiinteistövarallisuuden hallinnoinnista, kehittämisestä sekä valtion käytöstä poistuneiden kiinteistöjen myynnistä (senaatti). Senaatti-kiinteistöt on tietoturvallisuuden kannalta keskeinen yhteistyökumppani toimitilaturvallisuutta suunniteltaessa, sillä kiinteistöjen hallinnoijana he vastaavat niihin tehtävien muutosten toteuttamisesta.

Avarn Security on vartiointipalveluihin erikoistunut turvallisuusalan yritys ja se vastaa valtioneuvoston toimitilojen vartioinnista sekä aulapalveluiden tuottamisesta, ollen näin myös keskeinen yhteistyökumppani toimitilojen turvallisuuden toteuttamisessa.

3 Teoreettiset ja käsitteelliset lähtökohdat

3.1 Tietoturvallisuus

Tietoturvallisuuden historia alkaa jo ennen varsinaisen tietoteknisen vallankumouksen aikajakson alkua. Organisaatiot ovat aina olleet kiinnostuneita suojaamaan arkaluonteista tietoa, esimerkiksi liiketoiminnan puolella yrityssalaisuuksiin tai valtiollisella puolella varautumiseen liittyviä asiakokonaisuuksia (Zinatullin 2016, 2, Raggad 2010, 20). Tietotekniikka muodostaa siis vain yhden tietoturvallisuuden osa-alueen, joka tosin nykyaikana on hyvinkin keskeisessä roolissa.

Elinkeinoelämän keskusliiton (2016) mukaan tietoturvallisuus on turvallisuuden yksi osa-alue ja sen tärkeimmät suojattavat arvot ovat tietojen eheys, saatavuus ja luottamuksellisuus. Eheydellä tarkoitetaan, että tieto pysyy muuttumattomana tiedonkäsittelyn eri vaiheissa, saatavuudella tiedon käytettävyyden varmistamista ja luottamuksellisuudella sitä, ettei suojattava tieto päädy ulkopuolisten saataville. Näihin kolmeen tekijään kohdistuvat suojauskeinot vaikuttavat monesti negatiivisesti toisen tekijän suojaustasoon, esimerkiksi luottamuksellisuuden säilyttämiseksi kehitettävät suojaustoimet vaikuttavat monesti negatiivisesti tiedon saatavuuteen prosessien monimutkaistuessa (Zinatullin 2016, 2-4). Tiedon arkaluonteisuus vaikuttaa suojausmenetelmien painoarvoihin. Arkaluonteisimmissa tapauksissa korostuu tiedon luottamuksellisuuden säilyttäminen, kun taas julkisten materiaalien osalta korostuvat tietojen saatavuus ja eheys (Traficom, 2019).

Tietoja voidaan suojata joko teknisin tai hallinnollisin keinoin. Teknisillä keinoilla tarkoitetaan esimerkiksi tietoteknisiä laitteita, ohjelmistoja ja kohteen fyysistä suojausta. Hallinnollisilla keinoilla tarkoitetaan esimerkiksi politiikkoja, ohjeistuksia ja koulutuksia. Puhakaisen mukaan (2018, 5) toimivan kokonaisuuden aikaansaamiseksi on otettava huomioon inhimilliset tekijät, eli ihmisten on myös noudatettava annettuja ohjeistuksia ja määräyksiä. Hyvin suunnitellut järjestelmät ja tarkat ohjeistukset menettävät merkityksensä, mikäli niiden vaikutuspiirissä olevat työntekijät käyttävät niitä väärin tai toimivat ohjeistusten vastaisesti.

Tietoturvallisuus kattaa kaikki hallinnonalat ja on sidoksissa niihin muutoinkin, kuin vain turvallisuutta ohjaavana instanssina (Zinatullin 2016, 1). Jotta tietoturvallisuuden vaikuttavuus olisi mahdollisimman kattava, tulee kaikessa toiminnassa huomioida sidosryhmien merkitys kokonaisuuden muodostumisen kannalta. Jokaisen toiminnon tarpeet vaihtelevat toiminnan luonteen mukaan, jolloin myös organisaation eri toimijoilla suojattavien arvojen painotus saattaa muuttua riippuen käsiteltävän aineiston arkaluonteisuudesta (Zinatullin 2016, 13).

3.2 Organisaatiokulttuuri

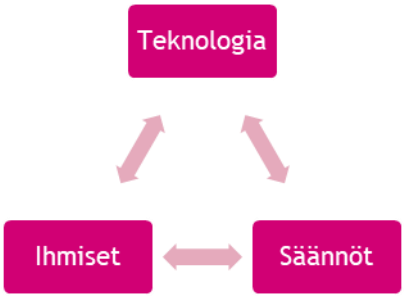
Puhakainen (2018, 3) toteaa Blogiin ja Datesiin viitaten, että kulttuuri on yhteisten uskomusten, arvojen, tapojen, käytöksen ja tuotteiden järjestelmä, jolla tietyn ihmisryhmän jäsenet

rakentavat suhdettaan maailmaan ja toisiinsa. Kulttuuri ohjaa ihmisten käyttäytymistä (Roer 2015, 9) ja sen eri syvyystasojen lisäksi ihmisten käyttäytymiseen vaikuttavat tilannetekijät kuten aikapaine, ja yksilökohtaiset tekijät, kuten persoonallisuus, tunnetilat väsymys ja kyvyt (Reiman, Pietikäinen & Oedewald 2008, 11).

Reiman, Pietikäinen ja Oedewald (2008, 10-11) toteavat Scheiniin viitaten (1985), että organisaatiokulttuuri on joukko henkilöstön jakamia ja yhdessä oppimia osittain tiedostamattomia oletuksia, jonka syvyystasot voidaan jakaa kolmeen luokkaan, perusoletukset, julkilausutut uskomukset sekä artefaktit. Perusoletukset ovat usein tiedostamatonta toimintaa ja niitä on vaikea havaita näkyvän käyttäytymisen seuraamisen perusteella, sillä monesti edes ryhmän jäsenet eivät tunnista niitä omassa käyttäytymisessään. Keskitaso eli julkilausutut uskomukset ovat esimerkiksi organisaation normeja tai filosofioita ja ovat näin helpommin havaittavissa. Kolmas taso eli artefaktit ovat esimerkiksi organisaatiossa käytettävä tekniikka, tuotteet ja siellä kerrotut tarinat ja ovat näin ollen kaikista helpoiten havaittavissa. Scheinin mallissa korostuu, että organisaatiokulttuuri on opittu malli ja niinpä sen muodostumiseen voidaan myös mahdollisesti vaikuttaa.

Bohnerin & Wänken mukaan ihmisten samankaltainen tapa suhtautua asioihin voi johtua eri tekijöistä tai tavoitteista. Esimerkiksi henkilö voi vastustaa sukupuolisyrjintää koska se estää etenemisen uralla (käytännön syy), koska se sotii vastoin hänen arvojaan tasa-arvon suhteen (arvopohjainen syy) tai koska muut hänen lähipiiristään vastustavat sitä (sosiaalinen syy). Ihmisten suhtautumiseen liittyvät tarkoitusperät eivät ole stabiileja, vaan voivat vaihdella tilanteesta riippuen, joten oikean vaikuttavan tekijän tunnistamisen sijasta tärkeää on ymmärtää, että ihmisen tarkoitusperät voivat monitarkoituksellisia (Bohner & Wänke 2002, 9). Samaa lähestymistapaa voidaan käyttää myös tietoturvallisuuteen liittyvissä kysymyksissä, sillä heidän esimerkissään käyttämä sosiaalipsykologian näkökulma on yleisesti sovellettavaa tietoa.

Roerin näkemyksen mukaan kulttuuri muodostuu ihmisistä, säännöistä sekä teknologiasta, joka on havainnollistettu kuviossa 2. Kyse on näiden kolmen tekijän summasta ja ne vaikuttavat kaikki toistensa toteutumiseen. Ihmisillä tarkoitetaan organisaation työntekijöitä jotka tulkitsevat sääntöjä ja käyttävät teknologian eri välineitä työnsä suorittamiseen. Säännöillä tarkoitetaan kirjoitettuja sääntöjä kuten lait, politiikat ja ohjeistukset sekä kirjoittamattomia sääntöjä kuten etiikkaa, moraalisia koodeja ja yhteisiä näkemyksiä. Organisaatiossa toimimisen perus edellytys on, että työntekijöiden käyttäytymistä ohjaavat ja rajoittavat säännöt on viestitty sekä perusteltu riittävän selkeästi. Teknologialla tarkoitetaan kaikkea työn tekemiseen käytettyä välineistöä tietotekniikasta nitojaan, sekä mentaalisia malleja (Roer 2015, 6-23).



kuvio 2: Kulttuurin muodostuminen (Roer 2015, 6-23)

3.3 Turvallisuuskulttuuri

Reimanin, Pietikäisen ja Oedewaldin (2008, 3) mukaan turvallisuuskulttuuri on rajatumpi näkökulma ja tarkastelutapa organisaatiokulttuuriin ja voidaan nähdä monitasoisena ilmiönä, jossa yhdistyvät henkilöstön kokemukset ja näkemykset, työyhteisön sosiaaliset ilmiöt ja organisaation toimintaprosessit. Roerin (2015, 2) näkemyksen mukaan turvallisuuskulttuuri on organisaatiokulttuurin alakulttuuri ja sen tavoitteena on taata työntekijöille uhkista ja vaaroista vapaa työympäristö. Olemukseltaan turvallisuuskulttuuri on organisaation kykyä ja tahtoa ymmärtää millaista turvallinen toiminta on, ymmärtää millaisia vaaroja toimintaan liittyy ja miten niitä voidaan ehkäistä, toimia turvallisesti, ehkäistä vaarojen toteutumista sekä edistää turvallisuutta (Reiman, Pietikäinen & Oedewald 2008, 8-9).

Turvallisuuskulttuuri muodostuu organisaation määritellessä turvallisuuden varmistamisesta seuraavia toimintavaatimuksia ja rajoituksia ja vastatessa näihin toiminnassaan (Reiman, Pietikäinen & Oedewald 2008, 3) ja se voi vaikuttaa turvallisuuteen joko parantaen tai heikentäen sitä (Puhakainen 2018, 6).

Reiman, Pietikäinen ja Oedewald (2008, 4) toteavat hyvän turvallisuuskulttuurin muodostuvan seuraavista ominaisuuksista: henkilöstöllä on edellytykset suoriutua hyvin työstään, organisaatiossa turvallisuutta pidetään aidosti tärkeänä asiana, turvallisuus ymmärretään riittävän laajasti, toimintaan liittyvistä vaaroista ollaan tietoisia, turvallisuuden kehittämisestä koetaan vastuuta ja siihen koetaan voitavan vaikuttaa sekä perustyön riittävästä ymmärryksestä ja hallinnasta.

Tärkeää on myös muistaa, että taitojen kehittäminen vaatii monipuolisempaa lähestymistapaa koulutusten järjestämiseen, ei pelkkiä luentoja asiasta. Määrätietoisen ja selkeän koulutussuunnitelman luominen helpottaa oikeiden asioiden tekemistä, sillä prosessina kulttuurin kehittäminen syö paljon aikaa (Roer 2015, 1-3, 79). Zinatullinin (2016, 77) mukaan ei ole mitään yksittäistä tekijää joka määräisi yksilön käyttäytymistä ja tämän vuoksi turvallisuuskulttuurin kehittäminen vaatii jatkuvaa ylläpitävää, vahvistavaa ja luovaa työtä. Turvallisuuskult-

tuuria kehitettäessä on tärkeää pystyä osoittamaan työntekijöille uusien menetelmien ja ohjeistusten mukanaan tuomat hyödyt, se että niiden tarkoitus on suojata eikä haitata heidän työtään (Zinatullin 2016, 71).

4 Opinnäytetyön toteutusprosessi

Opinnäytetyöprosessi aloitettiin yhteisellä suunnittelupalaverilla alkukeväästä, johon osallisuivat valtioneuvoston kanslian puolesta kaksi valtioneuvoston kanslian valmiusyksikön tietoturvaryhmän jäsentä sekä oppinäytetyön tekijä. Suunnittelupalaverissa sovittiin opinnäytetyön tutkimuskysymykset karkealla tasolla, opinnäytetyön lopputuotokset sekä alustava aikataulu opinnäytetyön suorittamiseksi.

Opinnäytetyön vaatimusten ollessa selvillä karkealla tasolla, aloitettiin tutkimusaiheeseen tutustuminen kirjallisuuskatsauksella, jossa pyrittiin tarkentamaan annettujen tutkimuskysymysten viitekehystä sekä hankkimaan valmista teoriapohjaa ensimmäisen ja toisen vaiheen tutkimusten suunnittelemiseksi. Aiheen tarkka rajaaminen jo ennen varsinaisen tutkimuksen tekemistä on tärkeää, jottei aihe paisu liian laajaksi ja että annetut tutkimuskysymykset saadaan käsiteltyä riittävällä laajuudella (Hirsjärvi, Remes & Sajavaara 1997, 85).

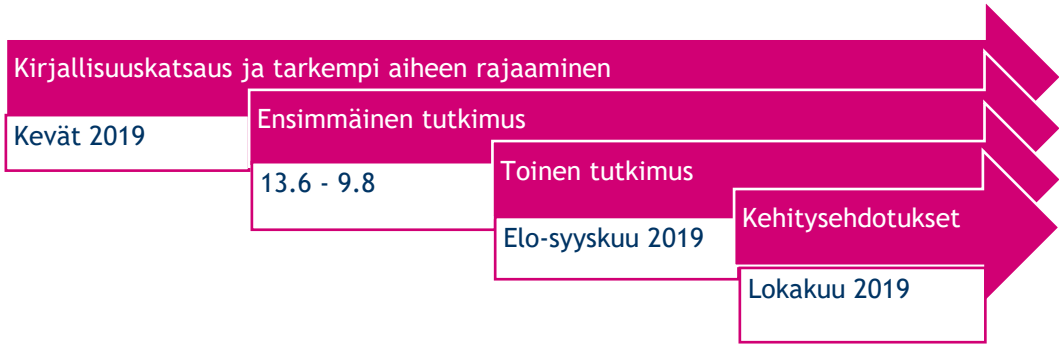
Kirjallisuuskatsauksen ohella suoritettiin riskiarvio opinnäytetyöprosessista ja mahdollisista esteistä sen toteuttamiseksi. Opinnäytetyön kannalta suurimmiksi riskeiksi arvioitiin riittävän kattavan tutkimusmateriaalin hankkiminen, aikataululliset haasteet, sekä opinnäytetyön julkisuuteen liittyvät haasteet, jotka käsitellään tarkemmin opinnäytetyön myöhemmissä vaiheissa.

Kirjallisuuskatsauksen jälkeen tarkennettiin tutkimuskysymykset, jotka olivat: mikä on valtioneuvoston kanslian tietoturvallisuuskulttuurin nykytila sekä mitkä ovat keskeiset kehityskohteet ja miten niitä tulisi kehittää. Tutkimuskysymysten tarkentamisen jälkeen rakennettiin opinnäytetyölle tutkimussuunnitelma, joka sisälsi aiheen tarkan rajauksen, teoreettisen viitekehyksen määrittelyn, tutkimusmetodien määrittelyn sekä koko opinnäytetyöprosessin karkean aikataulutuksen.

Varsinainen opinnäytetyö jakautui kolmeen vaiheeseen, joista ensimmäinen oli kaikille valtioneuvoston kanslian työntekijöille suunnattu kyselytutkimus, jonka tavoitteena oli selvittää kohderyhmä toisen vaiheen tarkempaa tutkimusta varten. Toisessa vaiheessa alkuperäisen suunnitelman mukaisesti oli tarkoitus pitää tarkentavia henkilökohtaisia haastatteluita ensimmäisen tutkimuksen analysoinnin perusteella havaituille poikkeaville ryhmille. Poikkeavia ryhmiä saattoivat olla esimerkiksi tietyt henkilöstöryhmät taikka osastot organisaation sisällä.

Kolmannessa vaiheessa kahden ensimmäisen vaiheen tuloksien perusteella muodostettiin tilannekuva sekä kehitysehdotukset. Tilannekuvan pohjana käytetään hyvin pitkälti ensimmäi-

sen vaiheen tutkimusta, jota täydennetään analyysivaiheessa toisen vaiheen tutkimuksen tuloksilla. Kehitysehdotusten pohjana käytetään molempia tutkimuksia, sillä siinä tehdyt havainnot ovat hyvin pitkälti organisaation toimintaan liittyviä haasteita. Opinnäytetyön kokonaisprosessi on kuvattu kuviossa 3.



kuvio 3: ONT prosessin aikataulu

Reimanin, Pietikäisen ja Oedewaldin (2008, 3) mukaan organisaation turvallisuutta arvioidessa on tärkeä huomioida kaikki kolme turvallisuuskulttuurin kolme tasoa, jotka ovat organisatoriset ja psykologiset ulottuvuudet sekä sosiaaliset prosessit. Organisatorisia sekä osittain psykologisia ja sosiaalisia tekijöitä pystytään arvioimaan ensimmäisen tutkimuksen perusteella. Toisella tutkimuksella pyritään tarkentamaan erityisesti psykologisia sekä sosiaalisia tekijöitä, jotka eivät ilmene ensimmäisen tutkimuksen tuloksissa.

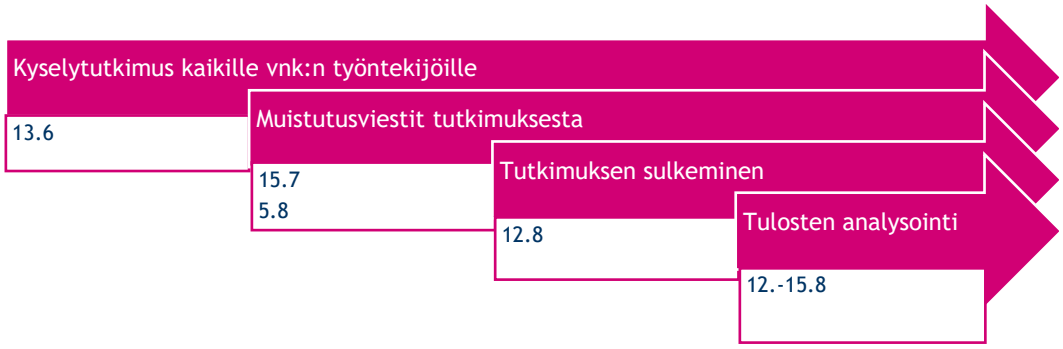
4.1 Koko organisaatiolle suunnattu kyselytutkimus

Tutkimusmateriaalin laajuuteen sekä aikatauluihin liittyviin haasteisiin vaikuttivat kesäkuun vaihteessa käynnistyvä hallituksen vaihdos, Suomen EU-puheenjohtajuuskauden aloitus heinäkuun alussa sekä kesälomakauden alkaminen juhannuksesta eteenpäin. Aikatauluihin liittyviin haasteisiin pyrittiin vastaamaan aikatauluttamalla ensimmäisen tutkimuksen julkaisu ennen kesälomakauden alkua, sekä jatkamalla sitä elokuun ensimmäiseen viikkoon asti.

Opinnäytetyön julkisuuteen liittyvät haasteet liittyivät tutkimuksista saatujen tulosten luottamuksellisuuteen sekä opinnäytetyön tulosten mahdollisesta turvallisuusluokittellusta. Luottamuksellisuuteen liittyvään haasteeseen pyrittiin vastaamaan anonymisoimalla kaikki tutkimukset, jolloin myös opinnäytetyön tekeminen helpottui osaltaan, sillä tutkimusmateriaalin vastauksista ei muodostunut tietosuojalain mukaista henkilörekisteriä. Ensimmäinen tutkimus

anonymisoitiin jättämällä tarkat henkilön tehtäviä ja roolia kuvaavat kysymykset pois tutkimuslomakkeelta, sekä käsittelemällä tietomassoja ainoastaan osastokohtaisilla taikka karkeilla roolikohtaisilla arvoilla.

Tutkimusaineiston laajuuteen liittyvään ongelmaan pyrittiin vastaamaan aikataulullisten tekijöiden lisäksi luomalla mahdollisimman helposti ja nopeasti vastattava tutkimus, jolloin vastaaja todennäköisemmin käyttää omaa työaikaansa sen suorittamiseksi. Ensimmäisen tutkimuksen tarkempi aikataulu on kuvattu kuviossa 4.



kuvio 4: Kyselytutkimuksen aikataulu

Ensimmäisessä tutkimuksen vaiheessa turvallisuuskulttuuria lähestytään Reimanin, Pietikäisen ja Oedewaldin (2008, 49) esittämän kuuden turvallisuuskulttuurin tekijän mukaan, sekä Roerin (2015, 6-23) esittämän kolmen näihin tekijöihin vaikuttavan osatekijän näkökulmasta, joista ihmiset on jaettu tässä tutkimuksessa esimiehiin sekä työntekijöihin. Mainitut näkökulmat asetettiin matriisiin, joka löytyy liitteenä 1. Jokaisen tekijän suhdetta verrattiin toisiinsa kuvion 5 mukaisesti ja niistä muodostettiin yksi tutkimuskysymys lomaketta varten. Näin ollen tutkimuskysymyksiä muodostui yhteensä 24. Tutkimuskysymykset käytiin läpi kokonaisuutena ja havaittuja puutteita täydennettiin viidellä lisäkysymyksellä.

kuvio 5: Esimerkki tutkimuskysymyksen luomisesta

Tutkimuskysymysten luomisen jälkeen tarkasteltiin järkevin lähestymistapa kysymysten pisteytysten ja kysymysasettelun osalta. Bohnerin ja Wänken mukaan ihmisten asenteet eivät ole suoraan havaittavissa, joten niiden arvioimiseksi on käytettävä jotain muuta menetelmää. Helpoin tapa on kysyä ihmisiltä suoraan heidän asenteistaan tutkittavan asian suhteen, joka on yleisesti kaikista käytetyin tutkimusmenetelmä. Tyypilliset kaksi eri vastausvaihtoehtoa sisältävät tutkimukset ovat nopeita toteuttaa, eikä niiden käsittely vaadi suurta vaivaa. Ongelmana näiden kohdalla on suuri polariteetti vastausvaihtoehtojen suhteen, joten mittaustuloksista ei saada monesti riittävän tarkkoja. Lisäksi kun vastaajat tietävät tutkimuskysymyksen sisällön ja mitattavan arvon, voivat he tiedostaen tai tiedostamatta ohjata vastaustaan siihen suuntaan minkä olettavat olevan positiivinen arvo (Bohner & Wänke 2002, 19-22).

Vaihtoehtoisena menetelmänä on rakentaa tutkimus niin, että haastateltava ei suoraan kysymysasettelusta ymmärrä, että tutkimuksessa mitataan hänen suhtautumistaan tiettyä arvoa kohtaan. Lisäksi kysymysten vastausvaihtoehtoja voidaan lisätä, jolloin vastauksiin saadaan lisää skaalautuvuutta ja näin ollen tutkimuksen tulokset ovat luotettavampia (Bohner & Wänke 2002, 19-22).

Tutkimuksessa päädyttiin yhdistämään suoria sekä skaalautuvia kysymyksiä, sillä kaikkien kysymysten osalta ei ollut mielekästä asettaa niitä skaalautuvaan asteikkoon, mutta toisaalta myöskään pelkillä suorilla kysymyksillä ei oltaisi päästy riittävän luotettavaan tutkimustulokseen. Tällöin myös tutkimuksen hyötysuhde saatiin korkeammaksi, kun tiedon keruu sekä analysointi nopeutuivat (Bohner & Wänke 2002,45). Lomakkeelle annettujen kysymysten lisäksi tutkimuksen lopussa vastaajille annettiin mahdollisuus antaa avoin vastaus joko tutkimuksen toteutukseen taikka muuhun tietoturvallisuuden aihepiiriin liittyen.

Tutkimuslomakkeessa (liite 2.) ensin vastaajista selvitettiin osasto jolla he työskentelevät sekä rooli jossa he toimivat, jotta tutkimustulosten analysointivaiheessa mahdolliset poikkeavat ryhmät pystyttäisiin tunnistamaan vastaajien joukosta. Osastoilla työskentelevien määrän

ollessa hyvinkin suuri, ei vastauksista pystynyt päättelemään vastaajan henkilöllisyyttä, pois lukien muutamien pienempien osastojen päällikön asemassa olevat henkilöt. Toisessa osassa vastaajille esitettiin kymmenen väittämää, joissa vastausvaihtoehdot olivat kyllä taikka ei. Kolmannessa osiossa esitettiin 19 väittämää, joissa vastausvaihtoehdot skaalautuivat yhden ja viiden välillä, 1 ollessa negatiivinen arvo, 3 neutraali ja 5 positiivinen arvo

Tutkimus päätettiin luoda verkkopohjaiselle lomakkeelle sen helpon jaettavuuden sekä tiedonkäsittelyn nopeuden vuoksi. Kehitetty tutkimuslomake luotiin Laurean tarjoamalle E-lomake verkkokysely alustalle, sillä työnantajalla ei ollut tarjolla vastaavaa, helposti saatavilla olevaa tutkimussovellusta. Tutkimuslomakkeen toimivuus testattiin pienellä koeryhmällä ja siitä saatujen tulosten perusteella muutaman kysymyksen asetteluun tehtiin pieniä muutoksia niissä kysyttävän tutkimuskysymyksen selkeyttämiseksi. Tutkimuskysymysten lisäksi tutkimuksen alkuun lisättiin lyhyt saateteksti, jossa käytiin läpi lomakkeen rakenne sekä luottamuksellisuuteen liittyvät tekijät.

Tutkimuslomakkeeseen tehtyjen viimehetken muutosten jälkeen lähetettiin tutkimuskutsu kaikille VNK:n työntekijöille valmiin sähköpostipostituslistan kautta, joka antoi välitystiedoksi 638 henkilöä. Tutkimukseen ohjaavan linkin lisäksi sähköpostiin lisättiin saatekirje (liite 3.) jossa vastaanottajille kerrottiin opinnäytetyön tekijän sekä oppinäytetyön taustat, opinnäytetyön aikataulu sekä tutkimuksen luottamuksellisuuteen liittyvät tekijät.

Ensimmäisellä tutkimuskutsukierroksella verkkolomakkeelle saatiin yhteensä 91- vastausta. Tutkimukseen kutsutuille lähetettiin muistutusviestit tutkimuksen puolessavälissä sekä viikko ennen tutkimuslomakkeen sulkemista, jotta sähköpostiviesteillä saavutettiin myös ne ketkä eivät työkiireiden taikka kesälomien vuoksi ennättäneet huomata ensimmäistä viestiä. Muistutusviesti lähetettiin alkuperäisen kutsun kanssa samassa viestiketjussa ja suppeammalla saateviestillä viittaamalla alkuperäiseen tutkimuskutsuun. Tutkimuslomake suljettiin suunnitellussa aikataulussa ja lopulliseksi vastaajamääräksi saatiin 130 henkilöä, joista 18 antoi vastauksen myös avoimen kentän tutkimuskysymykseen.

Tutkimuksen tulosten käsittely suoritettiin Excel-ohjelman avulla, sillä se mahdollistaa laajan aineiston tilastotieteellisen nopean käsittelyn. Tutkimuksen vastaukset saatiin E-lomakkeesta käsiteltäväksi suoraan Excel-tiedostona ja ennen niiden käsittelyn aloittamista tallennettiin alkuperäisestä tiedosta kopio tietoaineiston käsittelyn turvaamiseksi.

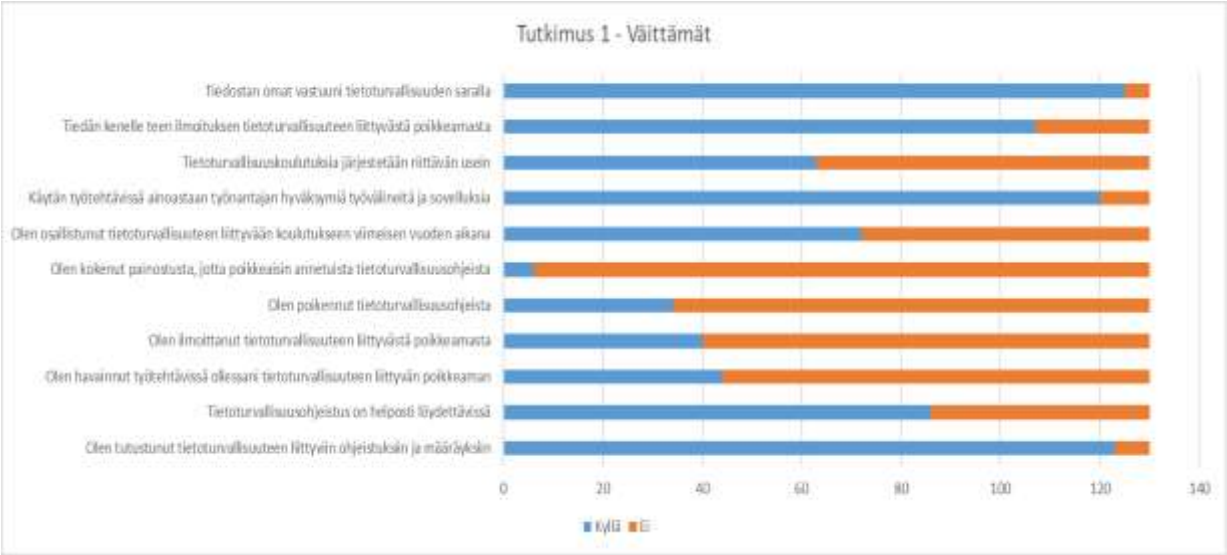
Tietoaineiston käsittelyn tavoitteena oli löytää vastaajien joukosta joko poikkeava henkilöstöryhmä, taikka osasto jota lähdetään tutkimaan toisen vaiheen haastatteluissa. Tämän toteuttamiseksi aineisto jaettiin kolmelle välilehdelle, joista ensimmäinen oli koko tutkimusaineiston, toinen osastotason ja kolmas roolitason analysointia varten.

Tutkimusaineiston käsittely aloitettiin Hirsjärven, Remeksen ja Sajavaaran (1997, 222) esittämän prosessin mukaisesti tarkastamalla tutkimusaineiston tiedot mahdollisten hylättävien vastausten löytämiseksi. Hylättäviä vastauksia ei löydetty ja kaikki vastaajat olivat täyttäneet lomakkeen kokonaisuudessaan, pois lukien viimeisen avoimen vastauskentän, johon vastaaminen oli jätetty tarkoituksella vapaaehtoiseksi. Seuraava vaihe aloitettiin analysoimalla VNK:n yleistilanne muodostamalla vastauksista graafiset pohjat lukujen hahmottamisen helpottamiseksi. Tutkimusaineisto analysoitiin tutkimuslomakkeen osioiden vastausjärjestyksessä, eli ensimmäisenä 1.osion väittämät, toisena 2. osion skaalautuvat kysymykset ja viimeisenä avoimen kentän vastaukset.

Väittämien tarkastelu suoritettiin kvantitatiivisesti muodostamalla jokaisesta tutkimuskysymyksestä oma kuvio. Tulosten selkeyttämiseksi väittämät on koottu opinnäytetyöhön yhdeksi kuvioksi. Tulosten analysoinnin yhteydessä havaittiin selkeitä kehityskohteita, varsinkin tietoturvakoulutusten sekä niiden jalkauttamisen osalta. Niin kuin kuviossa 6 on nähtävissä, tutkimukseen vastanneet henkilöt kokivat, ettei tietoturvallisuuteen liittyviä koulutuksia järjestetä riittävän usein. Todennäköisesti myös tästä johtuen osa henkilöistä ei ole osallistunut viimeisen vuoden aikana tietoturvallisuuden koulutuksiin. Tuloksista ei selviä, olivatko vastanneet henkilöt epätietoisia saatavilla olevasta verkkokoulutuksesta vai oliko kyse ennemminkin siitä, ettei verkkokoulutuksia haluta käydä.

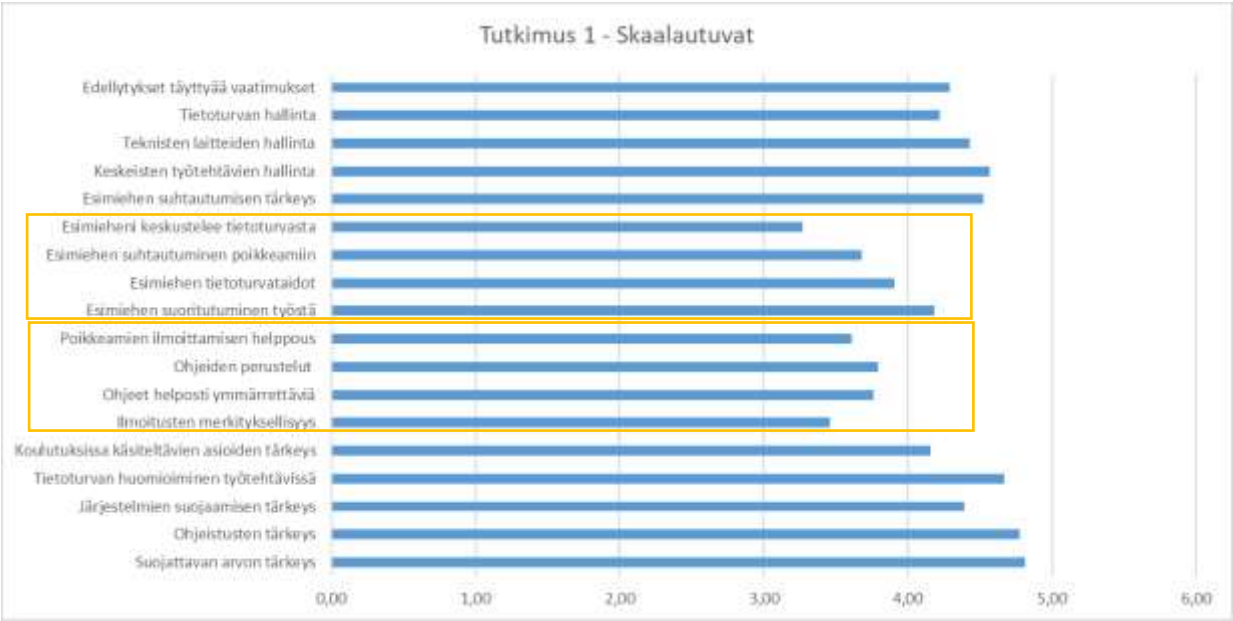
Mielenkiintoinen havainto kuviosta 6 on että ihmiset kokevat tiedostavansa omat vastuunsa tietoturvallisuuden saralla, vaikkakaan eivät ole osallistuneet siihen liittyviin koulutuksiin viimeisen vuoden aikana. Koulutuksiin osallistuminen on määritelty työntekijöiden vastuuksi (Tietoturvallisuuden hallinta valtioneuvostossa ja sen ministeriöissä, 2018, 5) ja näin ollen työntekijät joko eivät tiedosta omia vastuitaan taikka ovat tietoisesti poikenneet annetusta ohjeistuksesta.

Positiivisia havaintoja kuviosta 6 on, että valtaosa havaituista tietoturvapoikkeamista ilmoitetaan eteenpäin, ja pieni kolmen prosenttiyksikön erotus kyseisessä arvossa todennäköisesti johtuu siitä, etteivät kyselytutkimukseen osallistuneet ole tietäneet kenelle ilmoitus tulee poikkeamatilanteessa tehdä.



kuvio 6: Väittämien tulokset

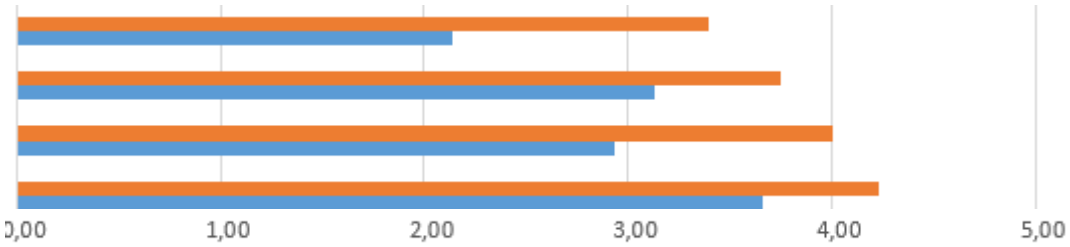
Toisessa vaiheessa käsiteltiin skaalautuvien kysymysten aineisto, joka yksittäisten kysymyskohtaisten kuvaajien sijasta käsiteltiin yhtenä koostavana kuviona. Organisaatiotasolla skaalautuvien tuloksia voidaan pitää suhteellisen hyvinä, sillä alhaisimmatkin arvot jäävät selkeästi positiivisen puolelle (kuvio 7). Selkeimmät erot skaalautuvien vastauksien joukosta olivat esimiestyö sekä tietoturvallisuusohjeiden selkeys, joka osaltaan on saattanut vaikuttaa kokemukseen siitä kuinka helposti poikkeamat ovat ilmoitettavissa, taikka kuinka merkittäväksi ilmoituksen tekeminen koettiin.



kuvio 7: Skaalautuvien tulokset

Tilastollisen analyysin lisäksi avoimen vastauskentän vastaukset käsiteltiin kvalitatiivisesti ja litteroitiin jatkokäsittelyä varten. Vastaukset litteroitiin kolmeen eri pääryhmään, jotka olivat koulutus ja sen kehittäminen, tekniikka sekä kyselytutkimuksen toimivuus. Avoimen kentän vastaukset otettiin huomioon toisen vaiheen haastattelukysymysten sekä kehitysehdotusten luomisen yhteydessä.

Osasto- sekä roolitason analyysi suoritettiin vertaamalla jokaisen ryhmän tuloksia organisaation keskiarvoon. Skaalautuvien kysymysten osalta pystyttiin havaitsemaan yksi poikkeava ryhmä, jossa organisaatiotason poikkeamaksi havaittu tekijä tuli vieläkin vahvemmin ilmi. Kuviossa 8, jossa oranssi linja kuvaa organisaation keskiarvoa ja sininen ryhmän vastausten keskiarvoa, on nähtävissä selkeä poikkeama. Ensimmäisen osuuden väittämiä analysoitaessa, tulokseen saatiin vahvistus ja näin ollen kyseinen ryhmä valittiin toisen vaiheen haastatteluiden kohteeksi.



kuvio 8: Esimerkki poikkeavan ryhmän tuloksista

4.2 Poikkeavalle kohderyhmälle suunnattu haastattelututkimus

Ensimmäisestä tutkimuksesta saadun tiedon perusteella tunnistettiin poikkeava ryhmä tietoturvallisuuskulttuurin osalta. Poikkeava ryhmä voi olla esimerkiksi henkilöstöryhmä taikka joku tietty VNK:n sisäinen osasto. Poikkeavan ryhmän tulosten arvoista oli havaittavissa organisaation keskiarvosta poikkeava tulos, joka on nähtävissä kuviossa 8.

Ensimmäisen tutkimuksen perusteella tunnistetuille ryhmille suunniteltiin alun perin pidettäväksi puoli-strukturoitu haastattelu, jonka laajuus ja sisältö määriteltiin ensimmäisessä tutkimuksessa tehtyjen havaintojen perusteella. Haastattelun tavoitteena oli vahvistaa ensimmäisen tutkimuksen perusteella tehtyjä havaintoja sekä päästä käsiksi ongelmien juurisyihin, joita ensimmäisen vaiheen pinnallisen tutkimuksen tuloksissa ei vielä olisi ilmennyt.

Haastattelua varten luotiin ensimmäisen tutkimuksen kanssa samassa aihepiirissä oleva kvalitatiivinen lomake. Tutkimuskysymykset pyrittiin rakentamaan valtioneuvoston koulutuksen yhteydessä esitetyn aktiivisen haastattelun mallin mukaiseksi niin, että osa kysymyksistä valmisteltiin etukäteen keskustelun ohjaamiseksi ja rajaamiseksi tietylle aihealueelle, mutta varsinaista keskustelua ja sen sisältöä rajoittamista pyrittiin välttämään. Metodin tarkoituk-

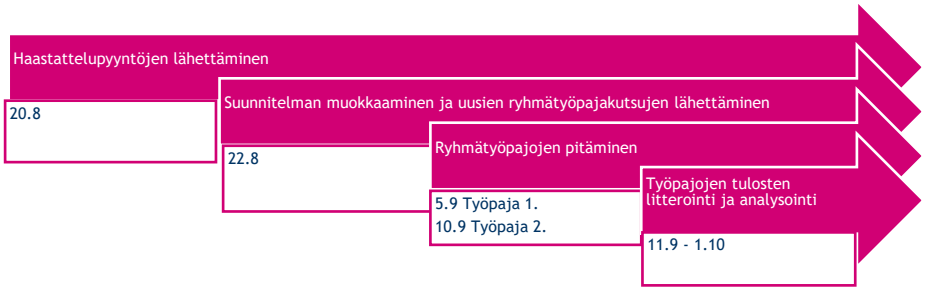
sena oli mahdollistaa ongelmien syvempi ymmärrys löytämällä ongelmien juurisyyt hyppäämättä suoraan johtopäätöksiin ensimmäisen tutkimuksen tulosten perusteella. Menetelmänä aktiivinen haastattelu on työläs ja aikaa vievä, joten se tulee toteuttaa pienemmälle tarkasti määritellylle kohderyhmälle (Saari, 2019). Tämän vuoksi tutkimukseen päätettiin haastatella korkeintaan kymmentä valitun kohderyhmän työntekijää.

Valmiiksi rakennettujen kysymysten lisäksi, ensimmäisen vaiheen löydösten perusteella ja resurssien niin salliessa haastattelussa suunniteltiin käytettäväksi interventiomenetelmää, joka esiteltiin valtioneuvoston laadullisten tutkimusmenetelmien koulutustilaisuudessa (Saari 2019). Menetelmässä rakennetaan väittämiä aiempien löydösten perusteella, joita esitetään haastateltaville ja vastausten lisäksi pyritään havaitsemaan haastateltavan reaktioita tunnetasolla, jolloin ilmiön syihin voidaan päästä tarkemmin kiinni.

Toisen vaiheen haastatteluiden prosessi aloitettiin hakemalla johtoon kuuluvalta henkilöltä lupa tutkimuksen toteuttamiseksi. Samalla hankittiin yhteystietoluettelo kyseisen ryhmän jäsenistä haastattelukutsujen lähettämiseksi. Kutsuun liitettiin uusi saatekirje, jossa käytiin läpi varmuuden vuoksi luottamuksellisuuteen liittyvät tekijät, aikataulu tutkimuksen osalta sekä eri vaihtoehdot tutkimuksen suorittamiseksi.

Haastattelupyyntöjen lähettämisvaiheessa alkuperäisen suunnitelman mukainen yksilöhaastattelu todettiin toimimattomaksi vaihtoehdoksi kohderyhmän aikataululllisten haasteiden vuoksi, jonka seurauksena suunnitelmaa muokattiin niin että henkilökohtaisten haastatteluiden sijasta pidettiin kaksi ryhmätyöpajaa. Tarkempi muokatun suunnitelman mukainen aikataulu kuviossa 9.

Ryhmätyöpajoja päätettiin pitää kaksi sijoittaen ne eri viikonpäiville, jotta mahdollisimman monella oli mahdollisuus osallistua niihin omien aikataulujensa puitteissa. Ensimmäiseen työpajaan osallistujia saatiin yhteensä 6 ja toiseen työpajaan 7, kokonaisosallistujamäärän ollen näin 36% kutsutuista.



kuvio 9: Tutkimuksen toisen vaiheen aikataulu

Ryhmätyöpajoissa päätettiin suunnitelman muuttumisesta huolimatta käyttää jo luotua kysymyslomaketta. Kysymyslomakkeen runkona toimivat myös ensimmäisessä tutkimuksessa käytetyt Reimanin, Pietikäisen ja Oedewaldin (2008, 48) esittämät kuusi turvallisuuskulttuurin tekijää sekä Roerin (2015, 6-23) esittämän kolmen näihin tekijöihin vaikuttavaa osatekijää, joita täydennettiin ensimmäisen tutkimuksen havainnoilla. Kysymyslomaketta ei julkaista osana opinnäytetyötä, sillä sen sisällöstä on suoraan pääteltävissä ensimmäisessä tutkimuksessa havaittujen poikkeamien luonne, sekä tilannekuvan yhden osion sisältö.

Ryhmätyöpajoissa päätettiin käyttää aiemmin mainittua aktiivisen kuuntelun menetelmää, jonka vuoksi tutkimuksessa tehtyjä havaintoja ei voitu kirjata suoraan muistiinpanoihin, sillä ilman erillistä kirjuria haastateltavien havainnointi kirjaamisen ohella ei olisi ollut mahdollista. Tämän vuoksi työpajat ja niissä käyty keskustelu päätettiin äänittää, josta tulokset ja tehdyt huomiot kirjattiin ja litteroitiin jälkeenpäin.

Työpajat aloitettiin kertaamalla opinnäytetyön tarkoitus, luottamuksellisuuteen liittyvät asiat mukaan lukien lupa äänittämiselle sekä haastatteluista saatujen tulosten käsittelyprosessi. Ryhmätyöpajat aloitettiin selvittämällä osallistujien roolit, sekä pääasiallinen työtehtävä jossa he toimivat. Tämän jälkeen heille esitettiin keskustelun avaava kysymys, jota tarvittaessa täydennettiin jatkokysymyksillä keskustelun edetessä. Molempien työpajojen osalta jatkokysymysten käyttöön ei ollut juurikaan tarvetta, sillä keskustelu ohjautui halutun mukaisesti oikealle aihealueelle, eikä keskustelun sisältöä toisaalta myöskään haluttu rajoittaa liikaa mahdollisimman monipuolisten havaintojen varmistamiseksi. Ryhmätyöpajojen lopuksi osallistujille näytettiin ensimmäisestä tutkimuksesta saadut tulokset, jonka ohella pyrittiin havaitsemaan heidän reaktiotaan tulosten laadun osalta.

Ensimmäiseen ryhmätyöpajaan osallistui 6 henkilöä ja toiseen 7 henkilöä. Osallistumisprosentti tehdylle kohderyhmälle oli hyvä suhteutettuna kutsuttujen määrään, mutta niiden tarkempaa kokoonpanoa taikka niihin osallistuneita henkilöstöryhmiä ei voida käydä läpi osana opinnäytetyötä, jotta tarkasteltu ryhmä, taikka sen jäsenet eivät ole pääteltävissä tutkimuksen tulosten käsittelystä.

Ryhmätyöpajojen toteuttamisen jälkeen niistä saadut äänitteet käsiteltiin kvalitatiivisin menetelmin. Äänitteet kirjattiin ensin tekstimuotoon lausetasolla, sekä sen jälkeen litteroitiin jatkokäsittelyä ja analysointia varten. Kvalitatiivisessa tutkimuksessa on tavoitteena ymmärtää tutkimuskohdetta ja sen keruussa käytetään saturaation käsitettä kuvaamaan aineiston riittävyyttä. Saturaatio saavutetaan, kun tutkimukseen osallistuvien haastateltavien vastauksissa alkaa ilmetä samat ongelmat. (Hirsjärvi, Remes & Sajavaara 1998, 181-183). Kahden työpajan litteroituja tuloksia verrattaessa, voidaan todeta saturaation saavuttaminen ainakin suurimpien havaittujen ongelmien suhteen. Suurimmat ongelmat liittyivät karkealla tasolla toimitilaturvallisuuteen, henkilöstön johtamiseen sekä koulutuksiin. Tutkimuksen tuloksia ei voida käydä tarkemmin läpi osana opinnäytetyötä VNK:n edustajan pyynnöstä.

4.3 Tilannekuvan muodostaminen

Opinnäytetyön julkaistavassa osassa käsitellään tilannekuvan teoreettinen perusta, mutta varsinainen tilannekuva rajataan opinnäytetyön ulkopuolelle. Tilannekuvan teoriatietoa käsiteltäessä törmättiin siihen, ettei sille ole olemassa yksiselitteistä määritelmää. Yhteistä aihetta käsittelevissä julkaisuissa kuitenkin oli sen päämäärä toimia päätöksentekoa tukevana työkaluna. Päätöksenteon tukemiseksi tilannekuvalla pyritään kartoittamaan ympäristössä tapahtuvia ilmiöitä, selvittämään niiden vaikutusta sekä arvioimaan niiden kehitystä tulevaisuudessa (Pew & Mavor 1998, 174).

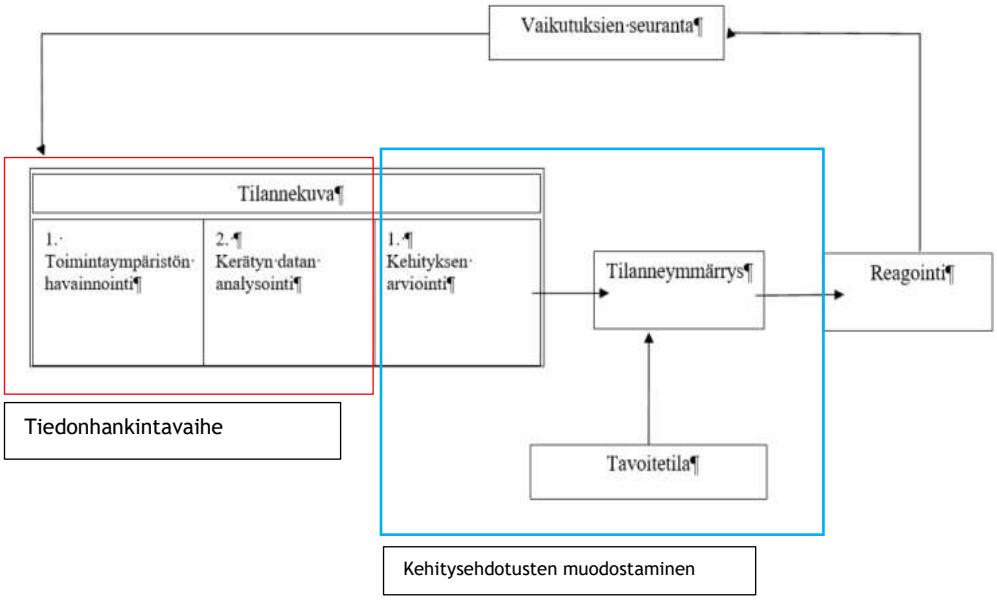
Pew ja Mavor (1998, 177) esittävät mallin jossa tilannekuvan käyttämistä osana päätöksentekoa tulee käsitellä jatkuvana prosessina. Prosessin ensimmäisenä vaiheena on nykyisen toimintaympäristön havainnointi, toisena vaiheena kerätyn datan analysointi ja merkitysten ymmärtäminen sekä kolmantena vaiheena tulevaisuuden kehityksen arviointi. Tilannekuvan ensimmäisen ja toisen osion syötteet (kuvio 10) saadaan opinnäytetyön kyselytutkimuksen sekä ryhmätyöpajojen analysoiduista tuloksista. Tulosten kehitystä pyritään arvioimaan kirjallisuuskatsauksesta saadun teoriatiedon perusteella, sekä tulevaisuudessa vertaamalla tuloksia edellisen vuoden tutkimukseen.

Tilannekuvan muodostumisen ja sen antaman informaation käsittelyn jälkeen muodostuu tilanneymmärrys (Kemppainen, 2019). Suhteuttamalla tilanneymmärrys haluttuun tavoitetilaan, saadaan selville tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Huomionarvoista on, että haluttujen päämäärien tulee olla riittävän tarkasti määriteltynä, sekä nykyisen tilanteen

analysoituna riittävän tarkasti. Toimenpiteiden suhteuttaminen ilman näiden tekijöiden tietämystä on mahdoton suorittaa, jonka seurauksena ne voivat olla joko yli- tai alimitoitettuja (Pew & Mavor 1998, 197).

Toimenpiteiden ollessa selvillä, tehdään päätös reagoinnista halutun lopputuloksen saavuttamiseksi. Päätöksen jälkeen seurataan sen aikaansaamat vaikutukset ja prosessi käynnistyy alusta. Varsinainen toimenpiteiden suorittaminen sekä niiden vaikutusten seuranta suoritetaan opinnäytetyön jatkoprojektina ja niiden sitominen osaksi opinnäytetyöprosessia on nähtävissä kuviosta 10.

Tilannekuvan ylläpitämiseksi, tulee sen kehittäminen ja tiedon kerääminen sitoa osaksi normaaleja työprosesseja. Vahti-ohjeen (2011, 27) mukaan tietoturvaraportointi on yksi keskeinen tietoturvallisuuden johtamisen mekanismi tarvittavien kehitystoimien tunnistamiseksi sekä tilannekuvan muodostamiseksi. Johdon tulee olla tietoinen tietoturvallisuuden tilasta ja vaikuttavuudesta, sekä pystyttävä tarvittaessa reagoimaan välittömiä toimenpiteitä vaativiin tilanteisiin.



kuvio 10: Tilannekuvan prosessi

Tilannekuvan muodostava valvonta ja raportointi suunnitellaan siten, että resurssit suunnataan tietoturvallisuuden kannalta merkityksellisimpiin prosesseihin, tietojärjestelmiin, tietovarastoihin sekä tietoturvallisuusohjeiden noudattamiseen. (Vahti 2011, 27). Tietoturvallisuuskulttuurin tilannekuvan osalta kerättävä data saadaan käyttämällä ja kehittämällä tässä opinnäytetyössä käytettyä tutkimuslomaketta. Uusi tutkimus tietoturvallisuuskulttuurin tasosta on hyvä suorittaa vuosittaisella tasolla, jolloin edellisellä kerralla päätetyt toimenpiteet ehtivät vaikuttamaan hitaasti muovautuvaan kulttuuriin.

5 Kehitysehdotukset

Kehitysehdotukset käsitellään kokonaisuudessaan osana opinnäytetyötä. kehitysehdotusten perustelut johdetaan ainoastaan ensimmäisen tutkimuksen tuloksista, sillä toisen vaiheen ryhmätyöpajojen tuloksia ei käsitellä osana opinnäytetyötä toimeksiantajan toiveesta.

5.1 Riskitietoisuuden kehittäminen

Organisaatiossa työskentelevät henkilöt vaikuttavat tiedostavan tietoturvallisuuteen liittyvät haasteet ja heillä on selkeä kiinnostus asiaa kohtaan, joka vastaa Valtiovarainministeriön havaintoja (2016, 27). Tietoturvallisuuteen liittyvät riskit ovat kuitenkin hyvin dynaamisia, jonka vuoksi puutteellinen koulutus näkyy henkilöiden riskitietoisuuden puutteina.

Riskit aiheutuvat tilanteista, joissa uhkat yhdessä haavoittuvuuksien kanssa tuottavat jonkun asteisia seurauksia. Uhkat esiintyvät yleensä toiminnan ulkopuolella, kun taas haavoittuvuudet ovat toiminnan sisäisiä heikkouksia. Uhkat ilman haavoittuvuuksia sen enempää kuin haavoittuvuudet ilman uhkia eivät kasvata riskiä. Tietoturvallisuuteen liittyvistä riskeistä ei päästä ikinä kokonaan eroon, mutta niiden tasoa pystytään hallitsemaan toiminnan suojelemiseksi (Valtiovarainministeriö 2016, 35-36,38).

Tietoturvallisuuteen kohdistuvien riskein hallinta vaatii riskien olemassaolon tiedostamista ja riittävän osaamispohjan luomista esimerkiksi koulutusten, ohjeiden ja käytännön jalkauttamisen kautta. Riskien hallitsemiseksi ensimmäinen vaihe näin ollen on tietoisuuden lisääminen ja osaamisen hankkiminen, jotta eri sidosryhmät pystyvät itsenäisesti vaikuttamaan riskien muodostumiseen. (Valtiovarainministeriö 2016, 44)

5.2 Koulutusmallin kehittäminen

Koulutusmallin kehittämiselle ilmenee selkeä tarve molempien opinnäytetyötä varten sekä aiemmin valtionhallinnossa tehtyjen tutkimusten osalta. Vahti-ryhmän teettämässä tietoturvabarometrissä (2016) tehtiin seuraavat havainnot. Tietoturvallisuudessa ja sen mahdollistamassa toiminnan digitalisaatiossa ei onnistuta ilman koulutusta ja ohjeistusta. Saadun tietoturvakoulutuksen ja –ohjeistuksen vähäinen määrä on mielenkiintoinen, mutta hälyttävä ilmiö. Koulutukseen ja ohjeistukseen panostaminen sekä julkishallinnossa, että kunkin organisaation tasolla on välttämätöntä. Julkishallinnon työntekijöiden turvallisuudentunne on korkealla tasolla huolimatta siitä, että koulutuksen ja ohjeistuksen määrä koetaan riittämättömäksi. Koulutuksessa ja ohjeistuksessa havaitut puutteet ja riskit on pyrittävä kääntämään osaamiseksi ja mahdollisuuksiksi (VAHTI-tietoturvabarometri 2016, 12-16). Vahti-ryhmän havainnot vastaavat tätä opinnäytetyötä varten toteutettujen tutkimusten tuloksia, joten myös heidän antamat kehitysehdotukset on syytä ottaa huomioon koulutusmallia kehitettäessä.

Katakri (2015) määrittelee koulutusvaatimukset seuraavasti. Suojattavan tiedon käsittelyn tehtäväkohtainen turvallisuuskoulutus annetaan henkilöstölle, joka käsittelee työssään suojattavia tietoja. Tehtäväkohtainen koulutus on räätälöity eri tehtäväryhmittäin. Koulutus on pakollinen käydä läpi ennen pääsyoikeuksien saamista suojattavien tietojen käsittely-ympäristöön. Koulutukseen osallistumista seurataan koulutusrekisterillä. Koulutus uusitaan vuosittain (Katakri 2015, 68.).

Koulutusten tulee vastata ihmisten odotuksiin niiden sisällön ja laadun suhteen. Ongelmat tässä voivat aiheuttaa vastaanottajassa kognitiivisen dissonanssin, eli poikkeaman ihmisen odotusten ja todellisuuden välissä, jolloin koulutuksen sisältö jää täysin huomiotta. Avaintekijänä onnistuneen koulutuksen suunnittelussa on tunnistaa yleisön pohjatiedot sekä tarpeet koulutettavan asian suhteen. Keskeisiin työtehtäviin kuulumaton sisältö, liian helppo taikka vaikeasti ymmärrettävä koulutussisältö vaikuttavat kaikki negatiivisesti koulutettavien motivaatioon ja oppimiseen (Roer 2015, 55).

Zinatullin (2016, 55) mainitsee Kirlappoksen, Beautementin sekä Sassen tekemän tutkimuksen, jonka mukaan syitä sille miksi ihmiset eivät seuraa ohjeistuksia on kolme, säännön noudattamiselle ei ole selkeää perustelua, säännön noudattaminen vaatii liikaa resursseja taikka sääntöä ei ole mahdollista noudattaa. Tietoturvakoulutuksissa käsiteltävä aihepiiri on käytävä läpi riittävän laajasti ja niiden tietoperusta on hyvä pohjata jo annettuihin määräyksiin ja ohjeisiin, jotta perusteet niissä käsiteltyjen aihepiirien osalta on varmasti hallussa. Menestyksellisen toiminnan jatkumisen kannalta on erittäin tärkeää, että organisaatiossa ymmärretään, miksi laadittuja tietoturvapolitiikkoja noudatetaan (Kettunen 2008, 14).

Yhteiskunnan, yhteisön, ryhmän ja organisaation määritelmiin sisältyy ajatus jaetuista arvoista ja moraalisesta järjestyksestä, jotka pitävät niitä koossa (Antikainen, Rinne & Koski 2013, 28). Mikäli koulutuksilla päästään vaikuttamaan näihin jaettuihin arvoihin, muodostuu organisaatiossa turvallisesta työskentelystä itseohjautuva tapa, jolloin myöskin henkilöstön motivaatio seurata annettuja ohjeita paranee.

Ihmiset antavat merkityksiä ja tekevät valintoja koulutuksen ja oppimisen pohjalta sen tilan puitteissa, jonka yhteiskunta ja koulutusrakenteet tarjoavat (Antikainen, Rinne & Koski 2013, 13). Oikeanlaisilla koulutusmetodeilla voidaan siis parhaassa tapauksessa päästä vaikuttamaan organisaatiossa työskentelevien henkilöiden tietoturvallisuuteen liittyvään päätöksentekoon. Esimerkkinä päätöksenteosta tilanne jossa henkilö tekee valinnan, sulkeeko hän työpäätteensä WC-tauon ajaksi, vai jättääkö hän työpöydän auki työnteon nopeuttamiseksi tauolta palattaessa.

5.3 Kulttuurin kehittäminen

Koulutuksia suunniteltaessa on huomioitava, että turvallisuustietoisuuteen liittyvä koulutus on vain yksi osa-alue turvallisuuskulttuurin muodostavassa kokonaisuudessa. Koulutuksia suunniteltaessa on otettava huomioon ihmiset, teknologiat sekä säännöt, jotta vaikuttavuudesta saadaan mahdollisimman kattava (Roer 2015, 34-35). Koulutusten sisällön suunnittelun lisäksi on tunnistettava tarvittavat sidosryhmät ja heidän roolinsa koulutusten suhteen (Roer 2015, 42)

Yleisesti ihmiset yrittävät noudattaa heille annettuja sääntöjä, mutta mikäli he kokevat sen perustyötä haittavana tekijänä, alkavat he luistaa niiden noudattamisesta. Satunnaisesti työntekijät saattavat tietoisesti olla noudattamatta annettua ohjeistusta, mutta tällöin juurisyynä monesti on ohjeistusten huono kohdentaminen työtehtävien vaatimuksiin (Zinatullin 2016, 60). Pienet väärinkäytökset tai piittaamattomuus ohjeiden noudattamisessa heikentää organisaation yleistä turvallisuuskulttuuria, jonka seurauksena tulevat suuremmat väärinkäytökset sekä yleinen piittaamattomuus ohjeiden noudattamisen suhteen (Zinatullin 2016, 72).

Rikkinäisten ikkunoiden teorian mukaan (Zinatullin 2016, 74) yksi säännöistä piittaamaton henkilö voi toiminnallaan saada aikaiseksi dominoefektin, lisäten myös vaikutuspiirissään olevien työntekijöiden piittaamattomuutta. Kyseinen teoria toimii myös päinvastoin, jolloin esimerkillinen sääntöjen noudattaminen saa myös muut työntekijät toimimaan samoin. Tämän vuoksi esimiesten osoittama esimerkki on keskeisessä asemassa turvallisuuskulttuurin kehittämisen kannalta. Ryhmähengen luominen ja kehittäminen on myös tärkeää, sillä vastakkainasettelut eri ryhmien kesken suuressa organisaatiossa vaikuttavat negatiivisesti yleiseen ilmapiiriin, joka taas heijastuu osaltaan turvallisuuskulttuuriin.

Keskiössä toiminnan tehokkuuden kannalta on nimenomaan esimerkillä johtaminen. Mikäli työntekijöissä ei saada herätettyä sisäistä motivaatiota, vaan sen sijasta heitä ajaa ulkoapäin suunnattu painostus, eivät he toimi halutun mukaisesti jatkuvasti, vaan ainoastaan valvonnan alla (kognitiivisen arvioinnin teoria, Zinatullin 2016, 83).

Henkilöstön käyttäytymistä ja sitä kautta organisaation kulttuuriakin tulisi pyrkiä ohjaamaan suuntaan, jossa henkilökunnan toimintatapa vastaisi mahdollisimman hyvin laadittuja tietoturvapolitiikkoja (Thomson &. Von Solms 2005). Tietoturvapolitiikojen tulisi pyrkiä vaikuttamaan organisaation työntekijöiden asenteisiin ja motivaatioon. Tilanteessa jossa organisaation henkilökunnalla on riittävästi tietoa tietoturvapolitiikoista, oikea asenne tietoturvaa kohtaan ja motivaatiota noudattaa politiikkoja, ohjeita tällöin myös pyritään noudattamaan (Paavilainen 1998, 84-85).

Antikaisen, Rinteen ja Kosken (2013, 33) mukaan yhteiskunta- ja arvojärjestelmän suuresta muutoksesta huolimatta ihmisten välinen vuorovaikutus perustuu edelleen normeihin, eli erilaisiin vuorovaikutuksen muotoihin, joiden välityksellä yksilöt oppivat toimimaan yhdenmukaisella tavalla. Normit voivat olla joko virallisia tai epävirallisia sääntöjä, määräyksiä, ohjeita tai suosituksia. Normien oikeutuksien perusta voi kiinnittyä virallisiin lakeihin ja määräyksiin, jolloin niiden kontrolli kuuluu viralliselle auktoriteetille. Toinen vaihtoehto normien perustan kiinnittymiselle on sosiaalisiin ja kulttuurillisiin rakenteisiin, jolloin ne eivät ole kenenkään asettamia, mutta voivat sitoa lakia tiukemmin.

Mikäli jo syntyneitä toimintamalleja pyritään muokkaamaan, tai etenkin rajoittamaan, vastustavat työntekijät sitä. Todennäköistä on, että muutos ei ohjaa ihmisiä käyttäytymään halutun mukaisesti vaan vaikutus on päinvastainen heikentäen tilannetta entisestään. Keskeistä suurien muutosten yhteydessä ovat selkeästi laaditut, toiminnan tuloksellisuuteen sidotut perustelut sekä johdon aktiivinen tuki (Zinatullin 2016, 31).

Tietoturvapolitiikojen noudattaminen on osittain riippuvainen myös organisaatiossa vallitsevasta ilmapiiristä. Työskentely tulehtuneessa ilmapiirissä voi aiheuttaa tietoturvapolitiikkojen tahallisia rikkomisia (Kettunen 2008, 13) Noudattaako organisaation henkilökuntaan kuuluva tietoturvapolitiikkoja vai ei, on useasti riippuvainen myös siitä, millaisen esimerkin organisaation johto ja työtoverit hänelle tarjoavat. Mikäli johdon toiminta ei vastaa politiikoissa määriteltyjä toimintatapoja, ovat ne käytännössä merkityksettömiä (Laaksonen, Nevasalo & Tomula 2006, 248-252).

Huolimatta ideaalityyppisestä tehokkuudestaan ja objektiivisuudestaan byrokratian on nähty myös esimerkiksi vähentävän ihmisen aloitteellisuutta työssään, sillä byrokraattisessa organisaatiossa kullekin virkamiehelle on määrätty tietty kompetenssin alue, jolla hän käsittelee asioita (Antikainen, Rinne& Koski 2013, 27). Byrokraattisen toimintaympäristön voidaan siis ajatella laskevan ihmisten oma-aloitteisuutta ja tämän estämiseksi tarvitsevat käyttäjät jatkuvaa tukea työkulttuurin ohjaamiseksi itseohjautuvampaan suuntaan.

5.4 Esimiestoiminnan tukeminen

Katakri (2015) määrittelee että turvallisuusohjeiden noudattamista ja ohjeiden muutostarpeita tulee arvioida säännöllisesti. Suojattavien tietojen käsittelyä koskevan koulutuksen tulee olla säännöllistä sekä uusille työntekijöille tulee antaa heti aloittamisen yhteydessä yleinen tietoturvakoulutus ja –ohje. Päivitetty tietoturvallisuuskoulutus tulee antaa koko henkilöstölle vuosittain ja siihen osallistuminen on pakollista (Katakri 2015, 68)

Valtioneuvoston määräyksessä tietoturvallisuuden hallinta valtioneuvostossa ja sen ministeriöissä (1110/70/2018) määritellään esimiesten vastuuksi seurata tietoturvallisuuskoulutuksien suorittamista vuosittaisella tasolla. Tutkimuksessa tehtyjen havaintojen mukaan tätä vastuuta

ei ole täysin täytetty, jonka seurauksena osa henkilöstöstä ei ole käynyt vaadittavia koulutuksia ajallaan.

Tutkimuksessa tehtyjen havaintojen mukaan tämä vastuiden laiminlyönti ei kuitenkaan ole seurausta välinpitämättömästä suhtautumisesta tietoturvallisuuteen liittyviä asioita kohtaan, vaan enemmänkin tietoisuuden puutetta omista vastuista. Ongelman ratkaisemiseksi tulee esimiehille suunnattua koulutusta kehittää ja kohdentaa tarkemmin työnasettamien vaatimusten täyttämiseksi.

5.5 Ohjeistusten käytettävyyden kehittäminen

Sääntöjä laativat henkilöt osaavat harvoin ottaa huomioon niiden aiheuttamia kuormitustekijöitä. Uusien sääntöjen noudattamisen vaatiminen ja työmenetelmien muuttaminen aiheuttavat monesti negatiivisen reaktion työntekijöiden keskuudessa, sillä ne nähdään ainoastaan aikaa ja energiaa kuluttavina rasitteina (Zinatullin 2016, 58).

Tietoturvapolitiikkojen rikkomuksista valtaosa johtuu yksinkertaisesti inhimillisistä erehdyksistä, tietämättömyydestä, huolimattomuudesta, kouluttamattomuudesta, välinpitämättömyydestä, motivaation puutteesta, vioista ja onnettomuuksista (Paavilainen 1998, 76-86). Valtaosan organisaation henkilöstöstä tulee noudattaa ja hyväksyä annetut tietoturvallisuusohjeet, sillä muuttamalla muutaman ihmisen käytöstä ei saada vielä aikaiseksi kokonaisuuden kannalta merkittäviä muutoksia (Puhakainen 2006, 69). Tietoturvallisuudesta annettavien ohjeiden ongelmana on kuitenkin se, että niitä monesti luodaan suurien ihmismassojen käyttöön, jonka seurauksena yksittäisten henkilöstöryhmien erityistarpeet saattavat jäädä huomioimatta. Jotta nämä henkilöstöryhmät ja heidän tarpeensa vähintäänkin tunnistetaan ohjeita luodessa, tulee ohjeita laativien henkilöiden jalkautua tehokkaammin eri henkilöstöryhmien keskuuteen tunnistaakseen heidän erityistarpeensa.

Tutkimuksessa havaittiin, että osa siihen vastanneista henkilöistä piti tietoturvallisuuteen ohjeita vaikeasti löydettävänä. Mikäli tietoturvallisuuteen liittyvät määräykset, politiikat ja ohjeistukset eivät ole helposti käytettävissä, todennäköisyys siihen, että ihmiset noudattavat niitä on erittäin pieni (Zinatullin 2016, 38). Tämän vuoksi myös ohjeiden käytettävyyden parantamiseksi tulee niiden jakamiskanava, taikka niistä viestiminen suunnitella uudestaan.

6 Pohdinta

Opinnäytetyön tavoitteena oli ensisijaisesti muodostaa tilannekuva tietoturvallisuuskulttuurin nykytasosta ja toisena tavoitteena antaa kehitysehdotuksia sen kehittämiseksi. Opinnäytetyölle asetetut tavoitteet saavutettiin suunnitelman mukaisesti, joskin tilannekuva vaatii vielä täydentämistä yksiköiden tietoturvallisuustason osalta, sekä visualisoinnin kehittämistä, jotta tuloksista saadaan esityskelpoisia myös tietoturvaryhmän ulkopuolisille tahoille.

Opinnäytetyön tiedonhankintavaiheessa toteutettuja tutkimuksia pystyttiin käyttämään tehokkaasti hyväksi kehitysehdotusten luomisvaiheessa ja niiden ansioista pystyttiin tunnistamaan selkeitä kehityskohteita, varsinkin toisen vaiheen ryhmätyöpajaan osallistuneen henkilöstöryhmän osalta. Kehitysehdotusten jalkauttaminen aloitetaan opinnäytetyön valmistumisen jälkeen valtioneuvoston kanslian osalta ja mikäli havaitut toimenpiteet koetaan tehokkaiksi ja toteutuskelpoisiksi, pyritään niitä käyttämään hyväksi myös koko valtioneuvoston tietoturvallisuuden kehittämisessä.

Vaikka tutkimuksista saadut tulokset olivat riittäviä kehitysehdotusten luomiseksi, eivät ne jälkeenpäin arvioituna mitanneet tietoturvallisuuskulttuuria syvällisellä tasolla, vaan ennemminkin hyvän tietoturvallisuuskulttuurin olemassaolon mahdollistavia tekijöitä. Mikäli kulttuuriin liittyvässä tutkimuksessa haluttaisiin mennä syvemmälle tasolle täytyisi tutkimusmenetelmiin lisätä esimerkiksi pelkästään havainnointiin keskittyviä tutkimusvaiheita, jolloin ihmisten sosiaalisiin prosesseihin ja pinnan alla tapahtuviin kulttuurin osatekijöihin päästäisiin paremmin kiinni.

Tutkimusaineiston kattavuus organisaatiotasolla oli riittävä, sillä 130 vastaajan aineistoa pystyttiin analysoimaan jo tilastotieteellisin menetelmin. Vastausprosentti oli alhainen (20,3%), vaikkakin verrattuna muihin valtionhallinnossa tehtyihin vastaaviin tutkimuksiin, esimerkiksi Vahdin toteuttamaan tietoturvabarometriin (2016) suhteutettuna sitä voidaan pitää jo suhteellisen hyvänä tuloksena. Tutkimuskutsut lähetettiin avoimella linkillä, sillä henkilökohtaisten linkkien lähettämiselle ei ollut mahdollisuutta E-lomakkeen kautta. Tämän vuoksi on mahdollista, että henkilöt ovat joko vahingossa, taikka tiedostaen vastanneet tutkimukseen useamman kerran. Tutkimuslomakkeen tulokset käytiin läpi karkealla tasolla, eikä täysin vastaavia vastausmalleja löydetty, joten todennäköisyys tälle on suhteellisen pieni.

Tutkimuksen validius (Hirsjärvi, Remes & Sajavaara 1997, 231) tietoturvakulttuurin mittaamiseksi on suhteellisen pitävä. Osat tutkimuskysymyksistä olivat monitulkintaisia riippuen vastaajan tietotaidosta tietoturvallisuuden suhteen, joka on saattanut vääristää ensimmäisen osuuden väittämien tuloksia. Esimerkiksi vastatakseen kysymykseen ”käytän ainoastaan työnantajan hyväksymiä sovelluksia ja laitteita”, tulee vastaajan tietää mitkä nämä hyväksytyt laitteet ovat. Mikäli vastaajalla on harhakäsitys hyväksytyistä laitteista vastaa hän kysymykseen oletettavasti väärin.

Ammatillisen kehittymisen näkökulmasta opinnäytetyö oli erittäin opettavainen kokemus. Työskentelyrutiinin osalta työtehtävien aikatauluttamiseen sekä kokousaikojen sopimiseen liittyvät haasteet havainnollistivat, ettei normaalityöelämä vastaa rytmitykseltään opiskelua juuri lainkaan. Opintojen aikana kokouksia suunniteltaessa tarvitsee ottaa korkeintaan huomioon viiden muun ryhmäläisen jo sovitut menot. Työelämässä toimintaympäristö on paljon laajempi ja jo sovitutkin ajat voivat peruuntua viime hetkillä. Tämä vaatii projektin vetäjältä

kärsivällisyyttä ja pidemmän tähtäimen suunnittelukykyä, muutoin projekti voi kaatua taikka lykkääntyä merkittävästi aikataulullisten haasteiden vuoksi.

Opinnäytetyön osana tehty kirjallisuuskatsaus auttoi syventämään turvallisuuskulttuuriin liittyvää tietämystä huomattavasti ja koen että se oli opinnäytetyön vaiheista yksi antoisimmista. Sanonnan mukaisesti tieto kasvattaa tuskaa ja tässä yhteydessä sen voisin kääntää niin päin, että uusi tieto kasvattaa avoimien kysymysten määrää. Avoimet kysymykset pakottavat ajattelemaan asioita uudelleen uudesta näkökulmasta. Näin ollen koen, että opinnäytetyön prosessi on osaltaan auttanut kypsyttämään työelämässä tarvittavaa kriittisen ja luovan ajattelun mallia yhä eteenpäin.

Lähteet

Painetut

Antikainen, A., Rinne, R. & Koski, L. 2013. Kasvatussosiologia. PS-kustannus, Jyväskylä.

Bohner, G. Wänke, M. 2002. Attitudes and Attitude Change. Psychology Press.

Herold, R. 2005, Managing an information security and privacy awareness and training program. Auerbach Publications, Boca Raton.

Hirsjärvi, S. Remes, P. & Sajavaara, P. 1997. Tutki ja kirjoita. Tekijät ja Kirjayhtymä

Kettunen M, 2008, Haastattelu tutkimus Verohallinnon tietoturvapolitiikkaohjeistuksien noudattamiseen vaikuttavista tekijöistä. Pro Gradu – tutkielma. Oulun yliopisto.

Laaksonen, M. Nevasalo, T & Tomula, K. 2006. Yrityksen tietoturvakäsikirja: Ohjeistus, toteutus ja lainsäädäntö, Helsinki: Edita Publishing.

Paavilainen, J. 1998. Tietoturva. Espoo: Suomen Atk-kustannus

Pew, R. & Mavor, A. 1998. Modeling Human and Organizational Behaviour. National Academy Press, Washington D.C.

Puhakainen P, 2006, A Design theory for information security awareness. Väitöskirja. Oulun yliopisto.

Puolustusministeriö, 2015, Katakri – Tietoturvallisuuden auditointityökalu.

Raggad, B. 2010, Information security management – Concepts and practice. CRC Press, Lontoo.

Reiman, T. Pietikäinen, E. Oedewald P. 2008.Turvallisuuskulttuuri – Teoria ja arviointi. VTT publications 700.

Roer K, 2015, Build a security culture, IT Governance Publishing.

Tietoturvallisuuden hallinta valtioneuvostossa ja sen ministeriöissä, 1110/70/2018.

Thomson, K. von Solms, R. 2005. Information Security Obedience: a Definition. Computers & Security.

Thomson, K & von Solms, R. 1998. Information Security Awareness: Educating Your Users Effectively. Infromation Management & Computer Security.

VAHTI. 2011. Johdon tietoturvaopas. Valtiovarainministeriö, Julkisenhallinnon ICT, Helsinki 2011.

VAHTI. 2016. Henkilöstön ja johdon tietoturvabarometri. Valtiovarainministeriö, Julkisenhallinnon ICT, Helsinki 2016.

Valtiovarainministeriö. 2016. Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi. Valtiovarainministeriö, julkisenhallinnon ICT, Helsinki 2016

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, 681/2010.

Valtioneuvoston ohjesääntö 3.4.2003/262

Valtioneuvoston kanslian asetus valtioneuvoston kanslian työjärjestyksestä 20.2.2015/162

Zinatullin L, 2016, The psychology of information security, IT Governance Publishing.

Sähköiset

Situation awareness. Psychologydictionary.org. https://psychologydictionary.org/situation-awareness/ Viitattu 17.10.2019

Tietoa Avarnista. Avarn Security. https://www.avarn.fi/avarn/ Viitattu 12.10.2019

Tietoa senaatista. Senaatti-kiinteistöt. https://www.senaatti.fi/tietoa-senaatista/ Viitattu 12.10.2019

Tietoa valtorista. Valtori. https://valtori.fi/tietoa-valtorista Viitattu 12.10.2019

Traficom. 2019. Pilvipalveluiden turvallisuuden arviointikriteeristö. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri.pdf Viitattu 12.10.2019

Valtioneuvosto ja sen tehtävät. Valtioneuvosto. https://valtioneuvosto.fi/tietoa Viitattu 2.6.2019

Valtioneuvoston kanslian tehtävät. vnk.fi. https://vnk.fi/ministerio/johto-ja-organisaatio Viitattu 2.6.2019

Valtioneuvoston kanslian asetus valtioneuvoston kanslian työjärjestyksestä. Finlex.fi. https://finlex.fi/fi/laki/ajantasa/2015/20150162 Viitattu 12.10.2019

Valtioneuvoston selvitys ja tutkimustoiminta. 2018. Kyberturvallisuuden strateginen johtaminen Suomessa. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf Viitattu 12.10.2019

Yritysturvallisuusmalli. Elinkeinoelämän keskusliitto. https://ek.fi/wp-content/uploads/yritysturvallisuus_2016.pdf Viitattu 17.10.2019

Julkaisemattomat

Powerpoint-esitys. Turvallisuuskulttuuri – rakentaminen, kehittäminen, johtaminen.13.11.2018. Petri Puhakainen.

Eveliina Saari. Luento – Laadullinen tutkimus yhteiskunnallisten ilmiöiden tulkkina. 27.5.2019

Sampo Kemppaisen haastattelu 17.10.2019

Kuviot

Kuvio 1: Valtioneuvoston kanslian organisaatio (valtioneuvoston kanslia) 8

kuvio 2: Kulttuurin muodostuminen (Roer 2015, 6-23)..... 11

kuvio 3: ONT prosessin aikataulu..... 13

kuvio 4: Kyselytutkimuksen aikataulu..... 14

kuvio 5: Esimerkki tutkimuskysymyksen luomisesta 15

kuvio 6: Väittämien tulokset..... 18

kuvio 7: Skaalautuvien tulokset 18

kuvio 8: Esimerkki poikkeavan ryhmän tuloksista..... 19

kuvio 9: Tutkimuksen toisen vaiheen aikataulu 21

kuvio 10: Tilannekuvan prosessi..... 23

Liitteet

Liite 1: Tutkimuskysymysten matriisi 36
Liite 2: 1.Tutkimuksen tutkimuslomake 37
Liite 3: Saatekirje 1. tutkimukseen..... 38

Liite 1: Tutkimuskysymysten matriisi

	Säännöt	Tekniikat	Työntekijät	Esimiehet
Henkilöstöllä on edellytykset suoriutua hyvin työstään	Kysymys 1	Kysymys 7	Kysymys 13	
Organisaatiossa turvallisuutta pidetään aidosti tärkeänä asiana	Kysymys 2	Kysymys 8		
Turvallisuus ymmärretään riittävän laajasti	Kysymys 3			
Toimintaan liittyvistä vaaroista ollaan tietoisia				
Turvallisuuden kehittämisestä koetaan vastuuta ja siihen koetaan voitavan vaikuttaa				
Perustyön riittävä ymmärrys ja hallinta				

Liite 2: 1.Tutkimuksen tutkimuslomake

Kyselytutkimus – Tietoturvallisuuskulttuuri valtioneuvoston kansliassa

Osio 1- Perustiedot:
Osasto jossa työskentelee:
- EU-asioidenosasto
- Omistajaohjausosasto
- Valtioneuvostonhallintoyksikkö
- Viestintäosasto
- Strategiaosasto
- Muu

Rooli:
- Asiantuntija
- Päällikkö
- Sihteeri
- Esimies
- Harjoittelija
- Muu

Osio 2 – Vastaukset Kyllä/Ei
Ohjeistukset:
- Olen tutustunut tietoturvallisuuteen liittyviin ohjeistuksiin ja määräyksiin.
- Tietoturvallisuusohjeistus on helposti löydettävissä
- Olen kokenut painostusta, jotta poikkeaisin annetuista tietoturvallisuusohjeistuksista

Arvot:
- Olen havainnut tietoturvallisuuteen liittyvän poikkeaman
- Olen ilmoittanut tietoturvallisuuteen liittyvästä poikkeamasta.

Tekniikka:
- Käytän työtehtävissä ainoastaan työnantajan hyväksymiä työvälineitä ja sovelluksia

Koulutus:
- Olen osallistunut tietoturvallisuuteen liittyvään koulutukseen viimeisen vuoden aikana
- Tietoturvallisuuskoulutuksia järjestetään riittävän usein
- Tiedän kenelle teen ilmoituksen tietoturvallisuuteen liittyvistä poikkeamista
- Tiedostan omat vastuuni tietoturvallisuuden saralla

Osio 3- Skaalautuvat (1-5) kysymykset
Arvot:
- Tietoturvallisuus on tärkeä suojattava arvo
- Tietoturvallisuusohjeistukset ovat tärkeitä
- Tietojärjestelmät tulee suojata tehokkaasti, vaikka se hidastaisikin niiden käyttöä
- Tietoturvallisuuden huomioiminen kaikissa työtehtävissä on tärkeää
- Tietoturvallisuuskoulutuksissa käsiteltävät asiat ovat tärkeitä työtehtävieni kannalta
- Koen että tekemilläni tietoturvallisuuspoikkeama ilmoituksilla on merkitystä

Ohjeistukset
- Tietoturvallisuusohjeet ja määräykset on perusteltu riittävän hyvin
- Tietoturvallisuusohjeistukset ovat helposti ymmärrettävissä
- Tietoturvallisuuspoikkeamien ilmoittaminen on helppoa

Esimiestyö
- Mielestäni esimieheni suoriutuu työstään hyvin
- Esimieheni omaa riittävät tiedot ja taidot tietoturvallisuuteen liittyen
- Esimieheni ottaa ilmoitetut tietoturvallisuuspoikkeamat vakavasti
- Esimieheni keskustelee tietoturvallisuuteen liittyvistä asioista aktiivisesti
- On tärkeää, että esimiehet puuttuvat havaittuihin tietoturvallisuuteen liittyviin poikkeamiin

Tekniikka ja koulutus
- Hallitsen omat keskeiset työtehtäväni hyvin
- Osaan käyttää työssäni tarvitsemiani tietoteknisiä laitteita hyvin
- Osaan käyttää kaikkia työskentelyssä vaadittavia tietoteknisiälaitteita turvallisesti
- Omaan riittävät tiedot tietojen turvallisesta käsittelystä
- Minulla on hyvät edellytykset täyttää tietoturvallisuuden asettamat vaatimukset työtehtävissäni.

Osio 4 - Avoin kysymyskenttä
- Mitä muuta haluaisit tuoda ilmi tutkimuksen yhteydessä?

Liite 3: Saatekirje 1. tutkimukseen

Hei,

Suoritan työharjoittelua valtioneuvoston kanslian valmiusyksikössä, jonne teen myös kesän ja alku syksyn aikana opinnäytetyöni. Opinnäytetyön tavoitteena on kartoittaa tietoturvallisuuskulttuurin tasoa valtioneuvoston kansliassa ja se koostuu karkeasti kolmesta eri vaiheesta. Kyseinen tutkimus on osa ensimmäisen vaiheen yleistilanteen kartoitusta ja se kohdistuu kaikkiin VNK:n työntekijöihin. Toinen vaihe koostuu haastatteluista, joiden kohderyhmä tarkentuu ensimmäisen vaiheen tutkimusten perusteella. Kolmannessa vaiheessa tavoitteena on muodostaa VNK:n tasoinen tilannekuva tietoturvallisuuskulttuurin tasosta sekä havaita mahdolliset kehityskohteet.

Ensimmäinen tutkimuslomake on auki elokuun 12. päivään asti. Mahdolliset pyynnöt toisen vaiheen haastatteluun osallistumiseksi lähetetään elokuun toisella viikolla. Molemmat tutkimukset suoritetaan täysin luottamuksellisesti ja kaikki vastaukset anonymisoidaan, jotta vastaajien henkilöllisyys ole pääteltävissä tutkimuksesta syntyvästä tuotoksesta. Tutkimuksen tuloksia käytetään ainoastaan opinnäytetyön tekemiseksi eikä sitä jaeta ulkopuolisille tahoille.

Linkki ensimmäisen vaiheen tutkimukseen on lähetetty jokaiselle VNK:n työntekijälle sähköpostin välityksellä ja olisi hienoa, mikäli pystyisit uhraamaan muutaman minuutin ajastasi tutkimukseen vastaamiseksi! Kysely on erittäin suppea ja aikaa sen vastaamiseen menee noin 5 minuuttia.

Linkki tutkimukseen:

https://elomake.laurea.fi/lomakkeet/17131/lomake.html

Mikäli sinulle heräsi kysymyksiä tutkimukseen liittyen niin vastaan mielelläni sähköpostin tai puhelimen välityksellä! Yhteystiedot löytyvät alapuolelta.

Terveisin

Sami Pouttu

Korkeakouluharjoittelija

Valmiusyksikkö

Valtioneuvoston kanslia

Puhelin ----------