Hannu Vesa

POLIISIN TIETOJÄRJESTELMIEN TOTEUTTAMINEN PILVIPALVELUISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Vesa, Hannu
Poliisin tietojärjestelmien toteuttaminen pilvipalveluissa
Jyväskylä: Jyväskylän yliopisto, 2018, 68 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja(t): Rönkkö, Mikko

Tämän pro gradun aiheena on pilvipalveluiden käyttömahdollisuudet poliisin ST (Suojaustaso) -luokiteltuja tietoja sisältävien tietojärjestelmien alustoina. Tutkimuksen tavoitteena oli selvittää voidaanko poliisin tietojärjestelmiä Suomen lainsäädännön ja valtionhallinnon ohjeistuksien puitteissa toteuttaa erilaisissa pilvipalveluissa ja miten näitä lakeja ja ohjeistuksia tietojärjestelmien parissa työskentelevät asiantuntijat tulkitsevat ja soveltavat.

Tutkimus toteutettiin laadullisena tutkimuksena. Tutkimusmenetelminä käytettiin kirjallisen aineiston läpikäyntiä ja puolistrukturoituja asiantuntijahaastatteluja. Tutkimustuloksina esitetään, että poliisin tietojärjestelmiä ja ST-luokiteltuja tietoja olisi mahdollista viedä pilvipalveluihin tietyin edellytyksin. Nykyisin monet olettavat, että tämä ei ole mahdollista ja osittain tästä johtuen tällä hetkellä pilvipalveluita ei käytetä poliisin tietojärjestelmien alustana.

Oleellisin rajaus pilvipalveluiden käytölle on se, että poliisin tietojärjestelmiä ei voida toteuttaa niin, että ne sijaitsisivat Suomen ulkopuolella. Lisäksi tutkimuksessa havaittiin, että tietojen ST-luokituksista päätettäessä koetaan tapahtuvan yliluokittelua. Tietoja luokitellaan korkeammalle suojaustasolle kuin mitä välttämättä olisi tarpeen ja tämä vaikuttaa tietojärjestelmien kehittämiseen ja tietojen käsittelyyn ja säilyttämiseen niissä.

Asiasanat: pilvipalvelut, poliisi, suojaustasoluokiteltu tieto, tietojärjestelmät

ABSTRACT

Vesa, Hannu
The Implementation of Police Information Systems in Cloud Services
Jyväskylä: University of Jyväskylä, 2018, 68 p.
Information Systems, Master's Thesis
Supervisor(s): Rönkkö, Mikko

The subject of this thesis is the possibilities of using cloud services as a platform for police information systems that contain classified information. The objective of the research was to find out if it is possible to implement police information systems in cloud services in accordance with the Finnish laws and government directives, and how these laws and directives are interpreted and carried out by the experts working with the information systems.

The research was carried out as qualitative research. Research methods used were half-structured interviews and analysis of written materials. Research results are that police information systems and classified information could be taken in to cloud services, provided certain requirements are met. Nowadays many people assume it is not possible, and partly because of this cloud services are not used as a platform for police information systems.

The most important limit for using cloud services is that police information systems cannot be located outside of Finland. In addition the research discovered that people feel there is over-classification happening when the classification levels of information is being decided. Information is classified to a higher confidentiality level than what would be necessary and this affects the development of information systems, and handling and storing data in those systems.

Keywords: cloud services, police, classification levels, information systems

TAULUKOT

TAULUKKO 1 Tutkimuksessa läpikäydyt lait ja asetukset 36
TAULUKKO 2 Tutkimuksessa läpikäydyt POHA:n määräykset ja ohjeet..... 37
TAULUKKO 3 Tutkimuksessa läpikäydyt VAHTI-ohjeet 37
TAULUKKO 4 Muita tutkimuksesssa läpikäytyjä ohjeita ja työkaluja..... 38
TAULUKKO 5 Pilvipalveluiden käyttömahdollisuuksista haastatteluvastauksia 40
TAULUKKO 6 Tietojen yliluokittelusta kertovat haastatteluvastaukset..... 42
TAULUKKO 7 Yliluokittelun vaikutuksista kertovat haastatteluvastaukset..... 43
TAULUKKO 8 Lainsäädännön ja ohjeistuksien vaikutuksia koskevia vastauksia 46
TAULUKKO 9 Haastateltavien mainitsemat lait 48
TAULUKKO 10 POHA:n ohjeet ja määräykset 49
TAULUKKO 11 Pilvipalveluiden tietoturvaan kohdistuvia vaatimuksia..... 51
TAULUKKO 12 Eri tuotantomallien mahdollistamat tietoaineistot 53

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

TAULUKOT 4

SISÄLLYS 5

1 JOHDANTO 7

2 KIRJALLISUUSKATSAUS 10
2.1 Pilvipalveluiden määritelmiä 10
2.1.1 Pilvipalveluiden käyttöönottomallit 10
2.1.2 Pilvipalveluiden tasot 12
2.1.3 Yhteenveto määritelmistä 13
2.2 Pilvipalveluiden edut 13
2.2.1 Strateginen taso 14
2.2.2 Taktinen taso 15
2.2.3 Operationaalinen taso 16
2.2.4 Yhteenveto eduista 16
2.3 Pilvipalveluiden haasteet 17
2.3.1 Pilvipalveluiden tietoturva, tietosuoja ja yksityisyys 17
2.3.2 Pilvipalveluiden hankintapäätöksiin, suunnitteluun ja käyttöönottoon liittyviä haasteita 22
2.3.3 Yhteenveto pilvipalveluiden haasteista 24
2.4 Viranomaisten erityisvaatimukset tietojärjestelmille 25
2.4.1 Yleisesti julkisen sektorin erityispiirteistä 25
2.4.2 Käyttäjien valvonta ja kontrollointi 28
2.4.3 Käyttövarmuus 29
2.4.4 Yhteenveto viranomaisten vaatimuksista pilvipalveluille 29
2.5 Yhteenveto teoriakirjallisuuskatsauksesta 30

3 TUTKIMUSMENETELMÄT 32
3.1 Tutkimusmenetelmät ja niiden valinta 32
3.2 Haastattelututkimus 34
3.2.1 Haastateltavien valinta 34
3.2.2 Haastattelujen rakenne ja analysointi 34
3.3 Kirjallisten lähteiden valinta ja läpikäynti 35
3.3.1 Lait ja asetukset 35
3.3.2 Poliisihallituksen (POHA) esikunnan ohjeet ja määräykset 37
3.3.3 VAHTI-ohjeet 37

3.3.4 Valtionhallinnon muita ohjeita ja työkaluja 38

4 TUTKIMUSTULOKSET 39
4.1 Haastattelututkimus 39
4.1.1 ST IV luokiteltujen tietojen vieminen pilvipalveluihin on mahdollista 39
4.1.2 Tietoja yliluokitellaan 41
4.1.3 Lainsäädännön ja ohjeistuksien määrä ja muutokset voivat johtaa siihen ettei pilvipalveluiden käyttöönoton tiedetä olevan mahdollista 45
4.2 Kirjallisen aineiston läpikäynti 50
4.2.1 Lainsäädäntö 50
4.2.2 Ohjeistukset 51
4.2.3 Yhteenveto kirjallisesta aineistosta 56

5 POHDINTA 57
5.1 Reliabiliteetti 59
5.2 Validiteetti 61

6 JOHTOPÄÄTÖKSET 63

LÄHTEET 65

LIITE 1 HAASTATTELURUNKO 69

LIITE 2 KATAKRIN ST IV JA ST III VAATIMUKSIA 73

1 JOHDANTO

Tämän pro gradun aiheena on pilvipalveluiden käyttömahdollisuudet poliisin sellaisten operatiivisten tietojärjestelmien alustana joissa säilytetään ST (Suojaustaso) -luokiteltuja tietoja. Tutkimusaiheena on se, että mitä poliisin tietojärjestelmiä voidaan Suomen lainsäädännön ja valtionhallinnon ohjeistuksien puitteissa erilaisissa pilvipalveluissa toteuttaa. Tutkimus rajautuu tähän näkökulmaan eikä käsittele pilvipalveluita ja niiden tietoturvaa teknisten kysymyksien osalta. Tutkimuskysymys on:

Miten asiaankuuluvia lakeja, asetuksia, viranomaisohjeistuksia yms. tulkitaan ja sovelletaan pohdittaessa voidaanko jokin poliisin operatiivinen, ST-luokiteltuja tietoja sisältävä tietojärjestelmä toteuttaa pilvipalveluna jollain tietyllä pilvipalveluiden käyttöönottomallilla tai tasolla?

Aihe on ajankohtainen ja kiinnostava koska nykyään yhä useampia tietojärjestelmiä toteutetaan pilvipalveluissa niiden tarjoamien etujen vuoksi. Pilvipalvelut tarjoavat käyttäjilleen (yksityishenkilöt, yritykset, julkiset organisaatiot) skaalautuvasti sovelluksia, tallennustilaa ja alustoja (Paquette, Jaeger & Wilson, 2010, s. 245). Pilvipalveluita käytetään muun muassa tiedon tallentamiseen, jakamiseen, hallintaan ja louhintaan. Armbrustin, Foxin, Griffithin, Josephin, Katzin, Konwinskin ja muiden (2009, s. 19) mukaan tietojärjestelmät tulisi jatkossa kehittää pilvipalveluihin. Järjestelmien ja niiden rauta-alustojen tulisi skaalautua suurelle määrälle virtuaalikoneita ja käyttäjiä. Ohjelmistoissa tulee heidän mukaansa olemaan osia jotka ajetaan virtuaalikoneilla pilvessä ja osia jotka ajetaan käyttäjien koneilla ja jotka ovat jossain määrin käytettäviä vaikka yhteys pilveen hetkellisesti katkeaisikin. Pilvipalvelutoimialalla ja akateemisten tutkijoiden parissa ennustetaan, että vuoteen 2020 mennessä työskentely tapahtuu pääasiassa pilvipalveluissa olevilla sovelluksilla perinteisten työpöytäsovelluksien sijaan (Jones, Irani, Sivarajahm & Love, 2017, s. 20). Näiden seikkojen vuoksi poliisihallinnonalalla on tärkeää tietää, millaisten tietojärjestelmien ja käsiteltävien tietoaineistojen osalta pilvipalveluiden tarjoamia etuja voisi hyödyntää poliisin tietojärjestelmissä nykyistä enemmän ja missä tapauksissa nii-

den käyttö taas on mahdotonta lainsäädännön, valtionhallinnon ohjeistuksien yms. takia.

Poliisin ja muiden viranomaisten tietoaineistot luokitellaan nykyään tietosisältöjensä mukaan suojaustasoille ST I - IV. Tietoaineistojen käsittelylle asetetut velvoitteet määritellään Tietoturvallisuusasetuksessa (681/2010) ja VAHTI2/2010 ohjeessa. Tietoturvallisuusasetuksen 3. luvun 9 §:ssä määritellään suojaustasot seuraavasti:

> 1) suojaustaso I, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;
>
> 2) suojaustaso II, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;
>
> 3) suojaustaso III, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle;
>
> 4) suojaustaso IV, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.

Näihin suojaustasoihin liittyvät tietoturvatasot. Ne ovat perustaso ST IV, korotettu taso ST III ja korkea taso eli ST II ja ST I. Viranomaisten lisäksi tietoturvatasot koskevat tahoja, jotka käsittelevät tietoja viranomaisten toimeksiannosta. Yhteiskunnan elintärkeiden toimintojen kannalta kriittisiä viranomaisasiakirjoja käsitellessä noudatetaan vähintään ST III:n mukaisia vaatimuksia.

Julkisen sektorin tietojärjestelmien tietoturvan ajankohtaisuutta korostaa esimerkiksi Ruotsissa heinäkuun 2017 lopulla julkisuuteen tullut tietoturvaskandaali, joka johti muun muassa kahden ministerin eroon. Kokonaisuudessa oli kyse siitä, että Ruotsin valtion ajoneuvohallinnon (Transportstyrelsen) IT-palveluita, tietojen käsittelyä ja tallennusta oli ulkoistettu IBM:lle. IBM:n kautta tiedot oli taas ulkoistettu Tšekkeihin, jossa niihin ovat voineet päästä kahden vuoden ajan käsiksi IBM:n sikäläiset työntekijät, joista ei oltu ainakaan Ruotsin toimesta tehty minkäänlaista turvallisuusluokitusta. Vaarantuneita tietoja olivat olleet ainakin ajoneuvorekisteri kuvineen, osoite- ja omistajatietoineen sekä ainakin osa puolustusvoimien ajoneuvorekisteristä. Sotilaallisesti kiinnostavia

tietoja ovat olleet tiedot Ruotsin teiden ja siltojen kantavuuksista ja mahdollisuus selvittää lentolupakirjatietojen avulla ruotsalaisten hävittäjälentäjien kotiosoitteet.

Tässä pro gradussa yhtenä tutkimusmenetelmänä on perehtyminen aihepiiriä käsittelevään ohjeistukseen eli Kansalliseen turvallisuusauditointikriteeristöön (Katakri), VAHTI-ohjeisiin (Valtionhallinnon tietoturvallisuuden johtoryhmän luomat tietoturvaohjeet valtionhallinnolle) ja Viestintäviraston ja Poliisihallituksen (POHA) ohjeisiin ja suomalaiseen lainsäädäntöön. Tarkoitus on perehtyä näihin niiltä osin mitkä velvoittavat tai ohjaavat poliisin toimintaa. Toinen käytettävä tutkimusmenetelmä on puolistrukturoidut haastattelut. Haastateltavat ovat Keskusrikospoliisista, POHA:sta ja Viestintävirastolta. Haastateltavat henkilöt ovat tekemisissä poliisin tietojärjestelmien suunnittelun ja ylläpidon sekä tietoturva- ja tietosuoja-asioiden kanssa.

Tutkimuksen tuloksena syntyy käsitys niistä raameista, mitä lainsäädäntö, asetukset, valtionhallinnon ohjeistukset yms. sanovat siitä, millaisia tietojärjestelmiä voidaan pilvipalveluina toteuttaa. Vastaavasti samalla syntyy käsitys niistä seikoista, jotka estävät pilvipalveluratkaisut. Tutkimuksen tulokset tarjoavat merkittävää hyötyä varsinkin silloin, jos osoittautuu, että pilvipalveluita voitaisiin hyödyntää tietojärjestelmissä nykyistä laajemmin ja sitä kautta saavuttaa pilvipalveluiden tarjoamia etuja. Tutkimustulokset selkeyttävät tilannetta ja auttavat toimimaan lakien, asetuksien ja ohjeistuksien mukaan. Tietojärjestelmien kehitystyössä tulee pystyä perustellusti tunnistamaan sellaiset tietojärjestelmät ja niissä tallennettavat tietoaineistot, joita ei voida edes harkita pilvipalveluina toteutettaviksi. Tutkimuksen tulokset ja kirjallisuuskatsauksen sisältö tulevat todennäköisesti olemaan jossain määrin yleistettävissä myös muiden suomalaisten viranomaisten ja Länsi-Euroopan maiden poliisivoimien toimintaan. Toisaalta kuitenkin eri hallinnonalojen ja maiden erilaiset lait, ohjeet ja asetukset rajoittavat tulosten yleistettävyyttä.

2 KIRJALLISUUSKATSAUS

Tässä luvussa esitellään ensin erilaisia pilvipalveluiden määritelmiä. Toisena aiheena tarkastellaan pilvipalveluiden tarjoamia etuja eli syitä, joiden takia pilvipalveluita käytetään tai joiden takia niiden käyttöä harkitaan. Tämän jälkeen perehdytään pilvipalveluiden haasteisiin painottaen tietoturvaan, tietosuojaan yms. liittyviä näkökulmia. Viimeiseksi käsitellään viranomaisten erityisvaatimuksia tietojärjestelmille.

2.1 Pilvipalveluiden määritelmiä

Pilvipalvelut ovat käsitteenä moniselitteinen ja niistä on lukuisia eri määritelmiä. Tässä alaluvussa esitellään pilvipalveluiden käyttöönottomalleja ja tasoja, joille erilaiset pilvipalvelut yleensä luokitellaan. Lisäksi käsitellään näiden huomioimista pilvipalveluita koskevissa akateemisissa tutkimuksissa. Käyttöönottomallit ja tasot on oleellista tuntea pilvipalveluita käsitteleviä tutkimuksia lukiessa ja erilaisten pilvipalveluiden käyttöönottoa harkitessa, koska niiden välillä on merkittäviä eroja.

2.1.1 Pilvipalveluiden käyttöönottomallit

Pilvipalvelut voidaan luokitella neljään National Institute of Standard and Technologyn (NIST) määrittelemään käyttöönottomalliin sen mukaan, millainen suhde toimittajan ja asiakkaan välillä on ja millaista käyttötarkoitusta varten pilvipalvelu hankitaan. (Yang & Tate, 2012, s. 38, Gashamia, Chang & Park 2013, s. 2, Chou 2015, s. 2, Tripathi & Nasina, 2017, s. 40.)

1. **Julkinen pilvi** (Public Cloud) on se mihin pilvellä yleensä viitataan. Julkisen pilven omistaa ja sitä operoi itsenäinen toimija ja kenen tahansa on mahdollista päästä asiakkaaksi.

2. **Yksityinen pilvi** (Private Cloud) on organisaation sisäisesti ylläpitämä tai ulkopuolisen toimijan toimittama ja se on tarkoitettu vain organisaation itsensä käyttöön. Se voi tarjota organisaatiolle mm. turvallisuutta ja vikasietoisuutta.

3. **Yhteisöpilvi** (Community Cloud) on useiden organisaatioiden käyttöön jaettu pilvi. Nämä organisaatiot jakavat yhteisiä kiinnostuksen kohteita kuten tavoitteet, tietoturvavaatimukset ja politiikat. Tällaista pilveä voi hallinnoida joko jokin kolmas osapuoli tai jokin tai jotkin näistä organisaatioista yhdessä.

4. **Hybridipilvi** (Hybrid Cloud) on yhdistelmä kahdesta tai kolmesta edellä luetellusta käyttöönottomallista. Organisaatiot myös voivat jakaa pilvipalveluiden käyttönsä useisiin eri pilviin esimerkiksi strategisista syistä tai kyberturvallisuuden takia.

Näistä neljästä käyttöönottomallista julkinen pilvi on se, mihin pilvipalvelutermillä alun perin viitattiin. Muut ovat sen variaatioita, jotka jakavat samoja teknologioita ja palveluita. Hybridipilvi on näistä yleisimmin käytetty (Mohapatra, 2017, s. 14). Suuret organisaatiot hyötyvät yksityisistä pilvistä, jotka on tehty näitä organisaatiota varten ja joita niiden käyttäjät ja yksiköt käyttävät ja pienet organisaatiot taas hyötyvät käyttäessään jonkun palveluntarjoajan ylläpitämässä julkisessa pilvessä olevia palveluita (Tripathi & Nasina, 2017, s. 41). Eri käyttöönottomalleilla on kullakin omat etunsa ja riskinsä ja mikään niistä ei täytä kaikkia vaatimuksia erilaisissa käyttötarkoituksissa (Mutkoski, 2015, s. 405). Julkinen pilvi ei ole menestynyt hyvin julkisella sektorilla siihen liitettyjen tietoturvahuolien ja kontrollin menetyksen riskin takia vaan organisaatiot ovat päätyneet siihen, että valtion tarjoama yksityinen pilvi on paras vaihtoehto (Garcia & Chow, 2015, s. 2).

Tässä tutkimuksessa yksityinen pilvi ja yhteisöpilvi ovat keskeisiä, koska kuten tutkimustuloksista selviää, niin niissä voidaan tietyissä tilanteissa käsitellä ja tallentaa korkeamman ST-luokituksen tietoja kuin julkisessa pilvessä. Yksityinen pilvi käytännössä tarkoittaa tilannetta, jossa organisaation omassa konesalissa tai organisaatiolle dedikoidussa konesalissa tai palvelimilla pyöritetään organisaation omia tietojärjestelmiä pilvipalveluteknologioita hyödyntäen ja soveltaen. Tällainen tilanne on kuitenkin erilainen kuin nykytilanne, jossa monet poliisin tietojärjestelmät ovat omissa palvelimissaan ja niin että kullakin järjestelmällä on vain muutamia järjestelmänvalvojatunnukset omaavia ylläpitäjiä. Toisaalta myös yhteisöpilvi, jossa olisi poliisin lisäksi myös muiden (turvallisuus)viranomaisten tietojärjestelmiä olisi ainakin teknisesti mahdollinen toteuttaa.

2.1.2 Pilvipalveluiden tasot

Pilvipalveluita voidaan tarkastella myös jaottelemalla niitä eri tasoille. Tasot kuvaavat sitä, mikä osa tietojärjestelmästä ja sen resursseista toteutetaan pilvipalvelutarjoajan toimesta ja mikä osa taas on asiakkaan itsensä toteuttamaa. Tasot vaikuttavat myös siihen mistä tietoturvan osa-alueista huolehtimiseen pilvipalveluiden toimittaja fokusoituu. NIST:in malli pilvipalveluiden käyttöönottomalleista ja tasoista on laajasti hyväksytty. Julkishallinto, yksityinen sektori ja tiedeyhteisö omaavat pääsääntöisesti yhteisen käsityksen tästä mallista (Garcia & Chow, 2015, s. 1). Pilvipalvelut luokitellaan NIST:in mallissa kolmelle tasolle (Yang & Tate, 2012, s. 38–39 , Gashamia ym., 2013, s. 2, Tripathi & Nasina, 2017, s. 40):

1. **Infrastruktuuriresurssipalvelussa** (Infrastructure as a Service, IaaS) tarjotaan skaalautuvasti laskentatehoa, tallennustilaa yms. resursseja Internetin välityksellä. IaaS:in käyttäjät hallinnoivat itse käyttöjärjestelmiään, tallennustilaa ja sovelluksia. Infrastruktuuria tarjotaan esim. vuosivuokralla tai käyttöön perustuvalla hinnoittelulla. Aroran ja Banerjin (2016, s. 2) mukaan tietoturvakäytännöt fokusoituvat IaaS:ssa virtuaalikoneiden luomiseen ja hallintaan.

2. **Alustaresurssipalvelu** (Platform as a Service, PaaS) tarjoaa ohjelmointi- ja suoritusympäristöjä. PaaS tuotteet toimivat integroituina suunnittelu-, kehitys-, testaus ja toteutusalustoina. PaaS:in käyttäjät voivat käyttää tuettuja ohjelmointikieliä ja rajapintoja ja julkaista ohjelmistojaan. He eivät hallinnoi pilven infrastruktuuria kuten verkkoja, palvelimia, käyttöjärjestelmiä tai tallennustilaa. Aroran ja Banerjin (2016, s. 2) mukaan tällä tasolla tietoturvassa on ensisijaista datan suojaaminen. Datan säilyttämistä koskeva lainsäädäntö ja säädökset sekä datan salaaminen ovat tärkeitä seikkoja.

3. **Ohjelmistoresurssipalvelu** (Software as a Service, SaaS) tarjoaa verkon välityksellä sovelluksia käytettäväksi avaimet käteen -periaatteella. Käytettävät ohjelmistot sijaitsevat pilvipalvelussa ja niitä käytetään selainten välityksellä. Tällöin ohjelmistoja ei tarvitse asentaa, suorittaa ja ylläpitää paikallisilla koneilla. SaaS käyttää multi-tenant arkkitehtuuria, jossa kaikki käyttäjät käyttävät samaa ohjelmakoodia. Autentikointia ja auktorisointia tarvitaan huolehtimaan eri käyttäjien tietojen pysymisestä erillään. Aroran ja Banerjin (2016, s. 2) mukaan tällä tasolla tietoturvafokus on sovellusten pääsynhallinnassa ja käyttäjien käyttöoikeuksissa eli siinä mitä he saavat sovelluksissa tehdä.

Näistä luokitteluista huolimatta pilvipalveluita tutkitaan yleensä erottelematta toisistaan erilaisia resurssipalvelutasoja (IaaS, PaaS, SaaS), käyttöönot-

tomalleja (julkinen, yksityinen, yhteisö ja hybridi) ja sitä millaista palvelua pilveen ollaan ulkoistamassa. Erilaisilla resurssipalvelutasoilla ja eri käyttöönottomalleilla on kuitenkin merkittäviä eroja jotka tulisi huomioida tutkimuksissa. Esimerkiksi SaaS:illa MS office 365:sta käyttävä henkilö tai organisaatio kohtaa paljon vähemmän riskejä ja saa pilvipalvelusta erilaisia hyötyjä kuin asiakas joka varastoi arkaluontoista dataa palveluntarjoajan pilvialustalle. Erilaisten pilvipalveluiden niputtaminen tutkimuksissa yhteen haittaa tulosten validiteettia. Esimerkiksi jos tutkimus on kohdistunut julkiseen pilveen ja SaaS:iin, niin sen tulokset eivät ole välttämättä yleistettävissä ja hyödynnettävissä käsiteltäessä yksityistä pilveä ja IaaS:ia. Tutkimukset olisivat hyödyllisempiä jos ne kohdistettaisiin tarkemmin esimerkiksi tiettyihin asiakkaisiin, resurssipalvelutasoihin tai käyttöönottomalleihin. (Haag, Echart & Krönung 2014, s. 2128–2133)

2.1.3 Yhteenveto määritelmistä

Yhteenvetona voidaan sanoa, että pilvipalvelut jaetaan neljään käyttöönottomalliin, jotka ovat julkinen, yksityinen, yhteisö- ja hybridipilvi (Yang & Tate, 2012, s. 38, Gashamia ym., 2013, s. 2, Chou 2015, s. 2, Tripathi & Nasina, 2017, s. 40.) ja kolmeen tasoon eli infrastruktuuri-, alusta- ja ohjelmistoresurssipalveluihin (Yang & Tate, 2012, s. 38–39, Gashamia ym., 2013, s. 2, Tripathi & Nasina, 2017, s. 40). Nämä käyttöönottomallit ja tasot ovat tärkeitä, jotta voidaan ymmärtää, että pilvipalvelu voi eri yhteyksissä tarkoittaa hyvin erilaisia palveluita. Tässä tutkimuksessa selvitetään, mitkä näistä tasoista ja malleista ovat tarkoituksenmukaisia Suomen poliisin tietojärjestelmiä pilvipalveluihin siirrettäessä ja ovatko jotkin niistä selvästi käyttöön soveltumattomia tämän tutkimuksen näkökulman puitteissa.

2.2 Pilvipalveluiden edut

Tässä luvussa esitellään etuja, joiden takia organisaatiot ja yksittäiset henkilöt voivat haluta ottaa pilvipalveluita käyttöön. Nämä seikat on oleellista tuntea, koska mahdollinen siirtyminen pilvipalveluiden käyttöön johtunee joistain niiden tarjoamista eduista.

Pilvipalvelut tarjoavat niitä käyttäville organisaatioille monia selviä etuja kuten parempi joustavuus, yhteentoimivuus, tietojen jaettavuus, pienempi energiankulutus, riskien siirtäminen (Haag ym., 2014, s. 2128–2133), päivitettyjen ohjelmistojen saavutettavuus, suurempi laskentateho ja suurempi tallennustila (Gashami, Chang, Rho & Park, 2014, s. 3). Pilvipalveluiden etuja on myös se, että niissä on nopeampaa toteuttaa pieniä tietojärjestelmiä ja että yhteydet Internetiä käyttäviin laitteisiin on helpompaa muodostaa. Lisäksi pilvipalveluiden etuja ovat parempi käyttövarmuus, halvempi hinta, parempi tietoturva, virtualisointitekniikoiden käyttömahdollisuus, resurssien ja kustannuksien ja-

kaminen, infrastruktuurin keskittäminen ja kapasiteetti kuormituspiikeistä suoriutumiseen. (Jones, 2015, s. 4.)

Edellä mainittuja pilvipalveluiden tarjoamia etuja voidaan tarkastella jaottelemalla ne strategiselle, taktiselle ja operationaaliselle tasolle. Strateginen taso liittyy luonteeltaan aineettomiin ja ei-taloudellisiin etuihin, joita pilvipalveluiden avulla voidaan saavuttaa. Operationaalinen taso käsittää etuja jotka ovat aineellisia ja taloudellisia. Taktinen ulottuvuus taasen käsittää niin aineettomia kuin aineellisiakin etuja kuten liiketoiminnan jatkuvuuden parantumisen ja nopeamman toimeenpanon. Nämä hierarkiatasot liittyvät perinteiseen jaotteluun ylimpään johtoon, keskijohtoon ja operatiivisella tasolla tapahtuvaan johtamiseen. Tarkastelu näillä tasoilla antaa uutta tietoa pilvipalveluiden eduista. Lisäksi se auttaa päätöksentekijöitä tekemään tietoon perustuvia IT:n investointipäätöksiä heidän arvioidessaan pilvipalveluiden käyttöönottoa erilaisissa tilanteissa. (Jones ym., 2017, s. 5)

2.2.1 Strateginen taso

Oikein toteutettu IT voi tarjota mahdollisuuden muuttaa organisaatiorakenteita ja liiketoimintaprosesseja tuottamalla merkittäviä organisationaalisia, teknisiä ja liiketoiminnallisia etuja. Informaation ja datan jakaminen eri organisaatioiden välillä mahdollistaa päätöksenteon joka perustuu täydellisempään informaatioon kuin jos tietoja eri organisaatioiden välillä ei jaeta. Esimerkiksi oikeusjärjestelmässä oikeusistuimet, lainvalvontaviranomaiset ja rangaistuslaitokset voivat jakaa tietojaan koordinoidakseen ja tehostaakseen toimintaansa. Tietojen jakaminen voi parantaa tuottavuutta ja päätöksentekoa ja vähentää kuluja. (Gil-Garcia, Chengalur-Smith & Duchessi, 2007, s. 121)

Strategisella tasolla pilvipalveluiden hyötyjä ovat Jonesin ym. (Jones ym., 2017, s. 5) mukaan seuraavat:

- Infrastruktuurin keskittäminen, joka mahdollistaa esimerkiksi halvemmat tilakustannukset.
- Käyttövarmuuden parantuminen, koska pilvipalveluiden käyttö vähentää riskiä, että yhden osan vioittuminen estäisi koko järjestelmän toimintaa.
- Laitteiden ja sijaintien itsenäisyys eli käyttäjät voivat päästä järjestelmään Internet-selaimen kautta riippumatta omasta sijainnistaan.
- Sisäisten IT resurssien vapautuminen muuhun käyttöön, kun käytetään enemmän ulkoisia resursseja.
- Mahdollisuus parempien palveluiden tarjoamiseen kansalaisille uusien liiketoimintamallien ja toimintatapojen avulla.
- Hiilijalanjäljen pienentäminen energiankulutuksessa säästämällä.

Strategisen tason etuna on myös se, että pilvipalveluiden käyttö vähentää tarvittavien palvelimien määrää ja siten se yleensä vähentää palvelimien virrankulutusta ja tarvittavan jäähdytyksen määrää. Täten pilvipalveluiden käyttö auttaa sopeutumaan vihreämmän energiankäytön globaaliin trendiin. (Li ym., 2015, s. 1.) Oleellinen kysymys laajemmassa mittakaavassa on se kuinka ihmiset vakuutetaan siitä, että pilvipalveluita kannattaa käyttää, koska niiden ekologiset vaikutukset voivat olla merkittäviä. Pilvipalveluita käytettäessä loppukäyttäjille hankittava tietotekniikka vie vähemmän tilaa ja sähköä ja on halvempaa kuin tilanteessa, jossa pilvipalveluita ei käytetä. (Gottschalk & Kirn, 2013, s. 13)

2.2.2 Taktinen taso

Pilvipalveluita tuottavat palveluntarjoajat hyötyvät suuruuden ekonomiasta monin tavoin ja osa näistä hyödyistä tulee heidän pilvipalveluitaan käyttäville asiakkailleen. IaaS:ia ja PaaS:ia käytettäessä asiakkaat hyötyvät myös siitä, että heidän on halvempaa ja helpompaa tarvittaessa vaihtaa pilvipalveluntarjoajalta toiselle (Vithayathil, 2017, s. 6).

Taktisella tasolla pilvipalveluiden hyötyjä ovat Jonesin ym. (Jones ym., 2017, s. 5) mukaan seuraavat:

- Liiketoiminnan jatkuvuus ja kyky toipua kriiseistä paranevat, kun palvelut toimitetaan useista eri fyysisistä sijainneista.
- Käyttäjät saavat lisää ketteryyttä ja voimaantuvat, kun he voivat itse uudelleen provisioida teknologisia infrastruktuuriresursseja.
- Uudet palvelut voidaan saada nopeammin käyttöön pilvipalveluiden kautta kuin perinteisillä järjestelmillä.
- Tietoturvaa ja -suojaa voidaan parantaa käyttäen hyödyksi pilvipalvelun tarjoajan tietoturvaan ja -suojaan erikoistuneiden työntekijöiden osaamista.
- Skaalautuvuus paranee, kun palvelimien ja tallennustilan käyttöä voidaan lisätä tai vähentää tarpeen mukaan.
- Sovelluksien siirtäminen fyysiseltä palvelimelta toiselle helpottuu.

Pilvipalveluiden tarjoajat voivat hoitaa tietoturvaa asiakkaidensa puolesta joiltain osin paremmin kuin nämä itse seuraavista syistä johtuen. Ensinnäkin pilvipalveluiden tarjoajien henkilökunta voi olla erikoistunut käytettyihin pilvi- ja tietoturvateknologioihin hyvin syvällisesti. Toisekseen palveluntarjoajille voi muodostua useiden asiakkaidensa kautta monipuolisempi ja syvällisempi näkemys erilaisista tietoturvaan liittyvistä asioista kuin niiden yksittäisille asiakasyrityksille. Pilvipalveluiden tarjoajilla on myös yleensä isot resurssit joista on hyötyä tietoturvan parantamiseksi. (Aikat, Akella, Chase, Juels, Reiter, Ristenpart ym., 2017, s. 61–62)

Hyvänä esimerkkinä tällaisista isoja resursseja omaavista toimijoista käyvät suuret pilvipalveluiden tarjoajat kuten Amazon ja Google, jotka ovat maailman suurimpia laitteistojen ja ohjelmistojen toimittajia. Näiden yrityksien pilvipalveluita käyttäessään asiakasorganisaatiot pääsevät hyötymään ajantasaisista tietoturvateknologioista. Palveluntarjoajat voivat myös tarjota tietoturvapäivitykset asiakkailleen keskitetysti. (Alassafi, Alharthi, Walters, & Wills, 2016, s. 30)

2.2.3 Operationaalinen taso

Operationaalisella tasolla pilvipalveluiden hyötyjä ovat Jonesin ym. (Jones ym., 2017, s. 5) mukaan seuraavat:

- Kustannukset pienenevät, kun investointien sijaan tulee yksikkökustannusmenoja.
- Organisaation sisäiset huolto- ja ylläpitokulut pienenevät ainakin IT-tiimien osalta, kun sovelluksia ei tarvitse asentaa kaikkien käyttäjien koneille ja niitä voidaan käyttää eri paikoista käsin.
- Työskentelykäytännöt ovat joustavampia, kun loppukäyttäjät voivat olla yhteydessä Internetissä olevaan pilvi-infrastruktuuriin mistä tahansa kunhan heillä on laite jolla pääsee Internetiin.
- Resurssien käyttö ja järjestelmien tehokkuus paranevat varsinkin sellaisissa tietojärjestelmissä, joita käytetään yleensä 10 - 20 prosentin teholla.
- Resursseja ja kustannuksia voidaan jakaa suuren käyttäjäjoukon kesken.
- Huippukuormien käsittelykapasiteetti paranee.

Pilvitallennuspalveluiden käyttäjät haluavat niiden tukevan katkeamatonta työskentelyä riippumatta siitä, mitä laitetta he käyttävät. Samaan dataan pitää olla mahdollista päästä käsiksi myös riippumatta käyttäjän omasta sijainnista. Dataa pitää myös pystyä tarpeen mukaan jakamaan ja synkronoimaan ja sitä pitää pystyä myös käsittelemään monipuolisesti työskentelytilanteen vaatimuksien mukaisesti. (Yang & Li, 2015, s. 9.) Mukavuus, tehokkuus ja saavutettavuus ovat seikkoja joiden takia pilvipalveluiden käyttöön voidaan haluta siirtyä (Gashami ym., 2014, s. 3).

2.2.4 Yhteenveto eduista

Kokonaisuutena voidaan perustellusti sanoa pilvipalveluiden käytön tarjoavan runsaasti erilaisia etuja organisaatioille ja käyttäjille. Monet näistä syntyvät pilvipalveluiden tarjoajien hyödyntäessä suuruuden ekonomiaa (Vithayathil, 2017, s. 6), infrastruktuurin keskittämistä ja virtualisointi. Pilvipalveluiden avulla mahdollisesti saavutettavissa olevia etuja ovat muun muassa hal-

vempi hinta, joustavuus, päivityksien jakelun helpottuminen, laiteresurssien jakaminen ja tehokkaampi käyttö, käyttövarmuuden paraneminen, riskien siirtäminen, tietojen jaettavuus ja saavutettavuus, tietoturvan mahdollinen paraneminen tietyiltä osin ja järjestelmien yhteentoimivuus. Pilvipalvelut nopeuttavat ja helpottavat erityisesti pienten tietojärjestelmien toteuttamista, kun ne voidaan toteuttaa suoraan olemassa olevaan pilveen ilman laitehankintoja yms. (Jones, 2015, s. 4.) Datan keskitetty tallentaminen helpottaa sen varmuuskopiointia ja hallintaa. Pilvipalveluiden käyttö voi vähentää tarvittavien palvelimien määrää ja tämä pienentää tarvittavaa fyysistä tilaa ja järjestelmien energiantarvetta. (Li ym., 2015, s. 1.) Yksi tapa tarkastella pilvipalveluiden tarjoamia etuja organisaatioiden johdolle eri tasoilla on jaotella ne strategiselle, taktiselle ja operationaaliselle tasolle (Jones ym., 2017, s. 6). Etujen ja käyttöönottoa tukevien syiden lisäksi tulee kuitenkin tarkastella myös pilvipalveluihin liittyviä haasteita.

2.3 Pilvipalveluiden haasteet

Tässä luvussa käsitellään pilvipalveluihin liittyviä haasteita ja syitä, miksi aivan kaikkea tietojenkäsittelyä ei aina kannata viedä pilveen, vaikka tarjolla olisikin luvussa 2.2 käsiteltyjä etuja. Lisäksi tarkastellaan asioita, jotka vaikuttavat halukkuuteen ottaa pilvipalveluita käyttöön. Nämä seikat on oleellista tiedostaa, jotta ymmärretään, miksi pilvipalveluiden käyttöönottoa kannattaa harkita useilta eri näkökulmilta. Pilvipalveluihin liittyviä haasteita ovat muun muassa teknologian monimutkaisuus ja kypsymättömyys sekä turvallisuusriskit, auditointistandardien puuttuminen ja sopimusasiat (Chou, 2015, s. 2–3).

2.3.1 Pilvipalveluiden tietoturva, tietosuoja ja yksityisyys

Pilvipalveluita käytettäessä tietoturvaan ja tietosuojaan kohdistuvien riskien katsotaan olevan suurempia kuin perinteisissä tietojärjestelmissä. Myös sääntelykysymykset ja datan säilyttäminen ulkomailla aiheuttavat huolta. (Whitley, Willcocks & Venter, 2013, s. 75–76) Erityisesti pitkäaikaiset tietoturvakysymykset aiheuttavat epävarmuutta organisaatioiden suhtautumisessa pilvipalveluihin (Shin, 2013, s. 196).

Pilvipalveluiden, kuten myös erillisinä toteutettujen tietojärjestelmien, tietoturvakäytäntöjen toteuttamisessa on hyödyllistä käyttää niiden tukemiseen, valvontaan ja auditointiin standardeja. ISO / IEC 27001 on nykyään yksi laajimmin hyväksytyistä tietoturvastandardeista. Se soveltuu hyvin erilaisten tietoturvallisuuskäytäntöjen toteuttamiseen ja arviointiin. (Li ym., 2015, s. 1.) Auditoinneissa tutkitaan toimiiko auditoinnin kohdeorganisaatio auditoitavien toimintojensa osalta sille asetettujen ohjeistuksien ja standardien mukaisesti. Auditoijat voivat olla organisaation sisältä tai ulkopuolisia tai näiden yhdistelmä.

IT-auditoinnit kohdistuvat yleensä johonkin tiettyyn aiheeseen, esimerkiksi tietokantaan, verkkoon, järjestelmäkehitykseen, tietoturvaan tai johonkin sovellukseen. Ne voivat kohdistua myös tietohallintoon tai pilvipalveluihin tai tietojärjestelmien käyttöön organisaatiossa. (Chou, 2015, s. 3)

Pilvipalvelualustojen käytössä valtionhallinnon kaltaisessa laajassa ja monimutkaisessa ympäristössä on erilaisia riskejä kuin keskitetyissä datakeskuksissa. Nämä riskit liittyvät muun muassa menettelytapoihin, dynaamisiin sovelluksiin ja dynaamisen ympäristön turvaamiseen. Tällöin tarvitaan uusia tietoturvakäytäntöjä turvallisen tietojenkäsittelyn mahdollistamiseksi. Seuraavia neljää kategoriaa voidaan käyttää mahdollisten riskien tunnistamiseen ja arvioimiseen pilvipalveluita käytettäessä (Paquette ym., 2010, s. 248–250):

1. Pääsynhallinta (Access). Organisaatioiden yksityisen datan tulee olla suojattua niin, että siihen pääsevät käsiksi vain he joilla on siihen oikeus. Jos yhdellä fyysisellä pilvipalvelualustalla säilytetään useiden asiakkaiden dataa, niin palveluntarjoajan tulee varmistaa, että kukin asiakasorganisaatio pääsee käsittelemään vain omaa dataansa. Jos pilvipalvelu toimii useissa eri maissa, niin datan yksityisyyttä ja tietoturvaa saattavat koskea useiden eri maiden lainsäädännöt.

2. Saatavuus (Availability). Oleellinen myyntivaltti pilvipalveluille on mahdollisuus tarjota 100 % saatavuutta asiakkaalle. Käytännössä katkoksia kuitenkin tapahtuu ja ne voivat olla hyvin kalliita asiakkaille. Pidempiä katkoksia voi aiheutua mm. ohjelmointivirheistä ja järjestelmien ylikuormittumisesta tai varajärjestelyjen puutteellisuudesta.

3. Infrastruktuuri (Infrastructure). Pilvipalvelu tulee suunnitella joustavaksi ja skaalautuvaksi. Pilvipalveluntarjoajan suorittama skaalaus ei kuitenkaan välttämättä toimi oikein isoissa järjestelmissä ilman asiakkaan panosta.

4. Eheys (Integrity). Datan tulee säilyä tarkasti oikein. Lisäksi on oleellista, että järjestelmän hallinnointiin, tehokkuuteen ja suorituskyvyn liittyvä informaatio on oikeaa.

Asiakkaiden tietojen yksityisyys on eettinen kysymys, koska organisaatio käyttää niitä hyväkseen saavuttaakseen tavoitteensa ja vaikuttaa sitä kautta asiakkaisiinsa. Yksityisyysnäkökulma voidaan laajentaa koskemaan myös työntekijöiden tietoja, sillä niiden voidaan nähdä olevan yhtä arkaluonteisia kuin asiakkaidenkin tietojen. Yksityisyydestä on tullut myös merkittävä laillisuuskysymys, jota koskevaa keskustelua teknologian jatkuva kehitys ylläpitää. Big Datan ja pilvilaskennan kehitys ovat monimutkaistaneet informaatioon ja yksityisyyteen liittyviä laillisuuskysymyksiä. Päätöksien tekeminen yksityisyydestä on organisaatioille yhtä haastavaa kuin se on yksilöillekin. (Pelteret & Ophoff, 2016, s. 291)

Organisaatioiden haasteet yksityisyyden parissa ovat todennäköisesti tiedonhallintaan, eettisyyteen ja lainsäädäntöön kuuluvia asioita sen sijaan että ne keskittyisivät vain yhteen näistä. Näihin haasteisiin vastaaminen riippuu hyvin monista asioista. Ensinnäkin organisaation tavoitteista, kulttuurista, strategioiden toteuttamisesta sekä siitä kuinka paljon sosiaaliset verkostot vaikuttava organisaatioon ja toimiiko se proaktiivisesti vai reaktiivisesti suhteessa ulkoisiin seikkoihin. Lisäksi vaikuttaa myös se mitä tietoja organisaatio kerää ja kerääkö se niitä innovaatioiden kehittämiseksi tai ymmärtääkseen asiakkaitaan. Organisaation toimintaan vaikuttavat myös sen havainnot siitä miten paljon asiakkaat arvostavat yksityisyyttään ja miten paljon organisaatio panostaa informaatioteknologiaan. Organisaatioiden, jotka näkevät yksityisyyden uhkana, tavoitteena on välttää ongelmia mukautumalla lainsäädäntöön ja vaatimuksiin. (Pelteret & Ophoff, 2016, s. 292)

Organisaatiot hallinnoivat Pelteretin ja Ophoffin (2016, s. 292) mukaan yksityisyyttä yksityisyysohjelmien kautta. Ne ovat kokoelma politiikkoja ja menettelytapoja joita toteutetaan asiakastietoja kerätessä, käytettäessä, turvattaessa, varastoitaessa ja hävitettäessä. Yksityisyyteen todella panostavat yritykset luovat lisäksi yksityisyyttä tukevan kulttuurin johtajuudella, koulutuksilla ja säännöllisillä auditoinneilla sekä pohtimalla yksityisyysnäkökulmaa aina kun ne alkavat käyttää arkaluontoisia tietoja jollain uudella tavalla.

Tilastojen mukaan yli puolet tietoturvaa uhkaavista tapahtumista johtuu organisaatioiden sisäpiiriläisistä D'Arcyn ja muiden (2009, s. 1) mukaan. Heidän nähdäkseen väärinkäytöksien suuri määrä osoittaa, että on tärkeää ymmärtää, kuinka tällaista käytöstä saataisiin vähennettyä. Ehkäisevän teorian mukaan sopivanlainen valvonta voi toimia tietojärjestelmien väärinkäytöksiä ennaltaehkäisevänä mekanismina nostamalla käyttäjien havaitsemaa uhkaa väärinkäytöksistä aiheutuvista rangaistuksista. D'Arcy ja muut esittävät laajennetun ehkäisevän teorian mallin, joka yhdistää kriminologiaa, sosiaalipsykologiaa ja tietojärjestelmiä. Mallin mukaan käyttäjien kohonnut tietoisuus tietoturvatoimenpiteistä ja väärinkäytöksistä seuraavien rangaistuksien todennäköisyydestä ja vakavuudesta vaikuttaa suoraan vähentävästi halukkuuteen väärinkäyttää tietojärjestelmiä. Mallin mukaan väärinkäytöksiä estävät seuraavat seikat: Käyttäjien tietoisuus tietoturvapolitiikoista, tietoturvakoulutus ja -harjoittelu ja tietotekninen valvonta. Tutkimustuloksien mukaan vaikuttaa siltä, että merkittävämpää ennaltaehkäisyssä on käyttäjien havainto väärinkäytöksistä aiheutuvien seuraamuksien vakavuudesta kuin väärinkäytöksistä kiinnijäämisen todennäköisyydestä. Pahantahtoisten sisäpiiriläisten toiminnan ehkäisemistä tutkineet Willisonin ja Warkentin (2013, s. 4) esittävät aihepiirissä tulevaisuudessa tutkittavaksi useita eri näkökulmia, jotka liittyvät mm. siihen miten sisäpiiriläisten väärinkäytöksiä voitaisiin ennaltaehkäistä vaikuttamalla heidän motivaatioihinsa ja mahdolliseen tyytymättömyyteensä, jota saattaa aiheutua siitä, jos he kokevat organisaationsa epäoikeudenmukaiseksi.

Pahantahtoiset sisäpiiriläiset eli organisaatioiden omat työntekijät ovat tietoturvallisuudessa merkittävä ongelma Willisonin ja Warkentin (2013, s. 1), D'Arcyn, Hovavin ja Gallettan (2009, s. 1) ja Cramin, Proudfootin ja D'Arcyn (2017, s. 1) mukaan. Sisäpiiriläiset ovat vahingollisia erityisesti siksi, että monet turvallisuutta parantavat ratkaisut on suunniteltu suojautumiseen ulkopuolisilta uhkilta (Vance, Lowry & Eggett, 2014, s. 2–3). Ulkopuolisia uhkia ovat mm. hakkerit ja luonnonkatastrofit. Organisaatioiden sisältä tulevilla hyökkääjillä on kuitenkin enemmän tietoja, resursseja ja käyttöoikeuksia kuin ulkopuolisilla hyökkääjillä, joten siksikin he muodostavat suuremman riskin kuin ulkopuoliset. Yleinen sisäpiiriläisistä aiheutuva uhka on käyttöoikeuksien rikkominen, joka tapahtuu, kun työntekijä käsittelee sensitiivistä dataa organisaation toimintatapojen vastaisesti. Mahdollisia syitä tällaiseen on monia: Petos, identiteettivarkaus, luottamuksellisen tiedon julkistaminen tai myyminen, tekijänoikeuksien alaisen materiaalin varastaminen ja harkitsematon uteliaisuus. Tällaiset rikkomukset ovat itsessäänkin vakavia ja ne asettavat organisaation alttiiksi syytteille, sanktioille ja mainehaitoille. Organisaatioiden tietoturvapolitiikat ovat perustavanlaatuinen lähestymistapa pahantahtoisten sisäpiiriläisten uhkaa vastaan. Tietoturvapolitiikoissa määritellään standardeja, rajoituksia ja vastuita käyttäjille ja tavoitteena on tukea tietoturvatapahtumien ehkäisyä ja havaitsemista sekä niihin reagoimista. (Cram ym., 2017, s. 1)

Edellä esiteltyjen tietoturvarikkomusten taustatekijöiden ymmärtäminen on oleellista sekä lyhyen aikavälin vaikutuksien mutta ennen kaikkea pitkän tähtäimen vaikutuksiensa vuoksi. Pitkällä aikavälillä tietoturvarikkomuksien vaikutukset kohdistuvat yhteiskuntaan. Jos ihmiset alkavat epäillä IT infrastruktuurin ja organisaatioiden kykyä heitä koskevan informaation turvaamiseen, niin se voi vaikuttaa lähes kaikkiin tietojärjestelmiä käyttäviin julkisiin ja yksityisiin toimijoihin. (Angst, Block, D'Arcy & Kelley, 2017, s. 20) Poliisihallinnon tietojärjestelmiä ja niiden kehittämistä varten on oletettavasti hyvin tärkeää, että kansalaiset luottavat tietojansa käsiteltävän niissä asianmukaisesti tietoturva ja -suoja huomioiden.

Tietoturva ja -suoja ovat Whitleyn ja muiden (2013, s. 76) mukaan huolehdittavia asioita paitsi toiminnan itsensä niin myös lainsäädännön noudattamisen kannalta. Lainsäädännön vaatimukset saattavat johtua maantieteellisestä tai liiketoiminnallisesta alueesta jolla toimitaan. Varsinkin alkuvaiheessa pilvipalveluiden käyttöönotto tarkoitti sitä, että tietojärjestelmät muuttuivat sisäisesti hallinnoiduista ja ylläpidetyistä erityisjärjestelmistä organisaation ulkopuolisiksi laitteisto- ja ohjelmistoalustahyödykkeiksi. Tätä muutosta perusteltiin hyvin usein kustannuksien vähentämisellä. Tämä johti usein siihen, että pilvipalveluiden asiakkaiden dataa ja tietojenkäsittelyprosesseja siirrettiin tarpeen mukaan alustalta toiselle, kuten pilvipalveluille on ominaista. Tällöin heräsi seuraavia kysymyksiä yksityisyydestä ja turvallisuudesta:

- Kuinka pilvipalvelun asiakkaat voivat olla varmoja, että heidän dataansa ei pääse käsiksi pilvipalvelua tarjoavan organisaation työn-

tekijät tai pilvipalvelun muut asiakkaat, joiden ohjelmistot ja data ovat samoilla alustoilla?

- Miten asiakkaat voi olla varmoja datansa peruuttamattomasta poistamisesta käytöstä poistettavilta tallennusmedioilta ja toisaalta siitä, että data on varmuudella tallessa lainsäädännön edellyttämän ajanjakson, joka on monesti useita vuosia?

- Kuinka asiakkaat voivat varmistua kriittisten järjestelmiensä osalta siitä, että palveluntarjoajan suunnitelmat häiriötilanteista toipumiseksi ovat riittävän tehokkaita?

- Onko riskinä, että pilvipalvelun toimittaja pyrkii lukitsemaan asiakkaan itseensä eli tekemään ratkaisuja, jotka tekevät tietojärjestelmien ja datan siirtämisen toisen palveluntarjoajan pilveen epäkäytännölliseksi tai mahdottomaksi?

- Mitä riskejä seuraa siitä, että samaa datakeskusta käyttävät useat eri asiakkaat? Tällöin on mahdollista, että yhteen asiakkaaseen kohdistuva palvelunestohyökkäys kohdistuu tahattomasti myös muihin saman datakeskuksen asiakkaisiin.

Vastaavasti pilvipalvelun tarjoajat kohtaavat samat ongelmat toisesta näkökulmasta. Eli miten he voivat suunnitella ja toteuttaa palvelunsa asiakkaiden tietoturvaan ja suojaan kohdistuvat huolenaiheet riittävän hyvin huomioiden ja myös vakuuttaa asiakkaansa siitä, että asiat ovat kunnossa. Ja miten vastuut tulee jakaa palveluntarjoajan ja asiakkaiden välillä. Lisäksi tulee huomioida se, että vaikka monet kysymykset kohdistuvat liiketoiminnallisista tarpeista johtuviin seikkoihin, niin datan yksityisyyttä koskevat huolet ovat monesti linkitettyjä myös suoraan tietojen käsittelyä ohjaavan lainsäädännön asettamiin vaatimuksiin. (Whitley ym., 2013, s. 76)

Tietoturvallisen pilvipalveluna toteutetun ympäristön tarjoamiseen liittyy edelleen avoimia kysymyksiä Alin, Khanin ja Vasilakoksen (2015, s. 379) mukaan, vaikka tiedeyhteisö on pyrkinyt niitä intensiivisesti ratkaisemaan. Ensisijaista olisi kehittää kattava ja integroitu turvallisuusratkaisu joka kattaisi useimmat merkittävät pilvipalveluiden tietoturvavaatimukset. Heidän mukaansa tutkimukset yleensä kohdistuvat yksittäisten tietoturvavaatimuksien ratkaisemiseen ja sitä kautta useiden eri ratkaisujen kehittämiseen vaikka käytännössä ei ole järkevää ja mahdollista, että tietoturvaa parantavia työkaluja olisi lähes yhtä monta kuin tietoturvavaatimuksia. Niiden käyttöönotto ja konfigurointi itsessään voi luoda riskejä. Pilvipalveluissa on oleellista hoitaa turvallisesti mm. pääsynhallinta ja identiteetinhallinta.

2.3.2 Pilvipalveluiden hankintapäätöksiin, suunnitteluun ja käyttöönottoon liittyviä haasteita

Tässä luvussa käsitellään pilvipalveluiden käyttöönoton harkintaan ja suunnitteluun liittyviä asioita kuten ulkoistuspäätöksien tekemistä ja palvelutasosopimuksia sekä sitä millaiset asiat vaikuttavat pilvipalveluiden käyttöönottohalukkuuteen.

Suuri osa sähköisen hallinnon pilvipalveluiden käytön tutkimuksesta on keskittynyt pilvipalveluihin liittyviin etuihin, huolenaiheisiin ja haasteisiin. Vähemmän tutkimusta on sen sijaan kohdistettu pilvipalveluiden käyttöönoton varhaisiin vaiheisiin eli arviointiin ja suunnitteluun. Arviointivaiheeseen kuuluvat pilvipalvelun käyttöönoton perustelut, tavoitteet ja yleiset ominaisuudet. Suunnitteluvaiheessa suunnitellaan koko prosessi pilvipalvelun käyttöönottoa varten. (Zhao, Gaw, Bender & Levy 2013, s. 43)

Pilvipalveluiden käyttöönottoa harkittaessa ja suunniteltaessa on huomioitava, että jos useiden organisaatioiden välisen tiedonjakamisen kehittämisprojektilta puuttuu selkeät tavoitteet tai niistä ei olla yksimielisiä, niin se vähentää odotuksia projektin tuottamasta hyödystä. Tällaisesta tilanteesta voi seurata että projektin johto epäonnistuu tavoitteiden artikuloinnissa ja että tavoitteet muuttuvat jatkuvasti ja että eri organisaatioiden väliset tavoitteet ovat keskenään ristiriitaisia. Jos projektin tavoitteet eivät ole selkeitä ja ne muuttuvat liian usein, niin se rajoittaa projektilla todennäköisesti saavutettavissa olevia etuja. (Gil-Garcia ym., 2007, s. 128)

Pilvipalveluun tietojärjestelmien siirtäminen on käytännössä ulkoistamista (varsinkin julkiseen pilveen siirryttäessä), joten IT:n ulkoistuspäätöksiin liittyvät kysymykset ovat osittain samoja joita harkitaan pohdittaessa pilvipalveluiden käyttöönottoja (Rajaeian, Cater-Steel & Lane, 2015, s. 1). Tietojärjestelmien ulkoistuspäätökset ovat hyvin monimutkaisia organisaatiollisia päätöksiä joihin liittyy organisaatioiden sisäisten tekijöiden lisäksi myös lukuisia ulkoisia tekijöitä. (Rajaeian ym., 2015, s. 9) Ulkoistamisen tavoitteena on monesti sen tarjoama mahdollisuus kustannussäästöjen saavuttamiseen ja joustavuuden lisäämiseen, mutta toisaalta se vaikuttaa myös päivittäiseen toimintaan ja sen hallinnointiin ja sillä on vaikutuksia myös strategisella tasolla (Ellram, Tate & Billington, 2008, s. 1).

IT:n ulkoistuksissa palvelun laatu ja hinta ovat kaksi merkittävää kysymystä (Aubert, Patry & Rivard, 1998, s. 8). Pilvipalveluiden hankintaan ja käyttämiseen liittyviä haasteita ovat mm. palvelutasosopimuksiin ja niiden toteutumisen seurantaan, datan yksityisyyden turvaamiseen ja tietoturvaratkaisuiden aiheuttamiin kustannuksiin liittyvät asiat. Palvelutasotasosopimuksia koskevia lakiasioita on vielä ratkaisematta. Lisätutkimusta vaatii palveluiden auditoiminen siltä osin, saavutetaanko luvatut palvelutasot vai ei. Toinen avoinna

oleva tutkimusalue on pilvipalveluiden sopimuksenmukaisen päälläoloajan varmistamisen mekaniikka. Kolmas on käytettyjen palveluiden hinnan laskeminen. Pilvipalvelutoimittajan antamat tilastot ja laskelmat eivät välttämättä ole kaikille tyydyttäviä ratkaisuja näihin kysymyksiin. (Ali ym., 2015, s. 379–380)

Yksi ulkoistamiseen liittyvä riski ovat piilokustannukset, joiden sanotaan joskus olevan isoin IT:n ulkoistamiseen liittyvä riski. Kustannuksia aiheutuu mm. palveluiden käyttöönotosta, uudelleenjärjestelyistä, kahden järjestelmän rinnakkaisesta käyttämisestä siirtymävaiheessa ja ulkoistettujen toimintojen valvonnasta ja niihin liittyvistä sopimusasioista. Kustannuksia syntyy jo sopivan pilvipalvelutoimittajan löytämisestä ja arvioimisesta ja myöhemmässä vaiheessa riitojen ratkaisemisesta. (Aubert, Patry & Rivard, 1998, s. 7)

Merkittävä haaste on myös datan yksityisyyden turvaaminen sen käsittelyn aikana. Kaikkia operaatioita ei voida toteuttaa, jos data on salattuna, jolloin sitä täytyy käsitellä selkokielisenäkin. Myös datan palauttaminen ja siirtäminen toiseen pilvipalveluun ovat aiheita jotka vaativat lisätutkimusta. On myös hyvä muistaa, että tietoturvaratkaisut luovat tarjoamiensa etujen lisäksi myös kustannuksia sekä pilvipalveluiden toimittajille että niiden käyttäjille. Turvallisuuden aiheuttamien kustannuksien ja pilven tarjoamien hyötyjen sekä turvallisuusvaatimuksien ja suorituskyvyn tasapainottaminen ovat oleellisia tutkimusaiheita. Näiden aihepiirien tutkiminen auttaa analysoimaan pilvipalveluiden käyttöön siirtymisestä saatavia hyötyjä ja aiheeseen liittyviä haasteita. (Ali ym., 2015, s. 379–380)

Joissain tapauksissa tietoturva- ja tietosuojavaatimukset nostavat pilvipalveluiden käyttöönoton hintaa ja toisaalta on huomioitava myös se, että toisinaan turvallisuushuolia saatetaan tarkoituksellisesti liioitella IT-osastojen toimesta, koska ne ovat haluttomia luovuttamaan kontrolliaan IT:sta (Whitley ym., 2013, s. 76). Toisaalta pilvipalveluiden käyttöön mukautuminen voi vahvistaa IT-osastojen roolia ja budjetteja kun taas sopeutumattomuus voi johtaa IT-osastojen kuihtumiseen. IT-osastot eivät ole pilvipalveluita käytettäessä enää monopoliasemassa olevia IT:n toimittajia organisaatioissaan vaan niiden roolina on kommunikoida sekä organisaation ulkopuolisten pilvipalvelutoimittajien että organisaation sisäisten tahojen ja loppukäyttäjien kanssa merkityksellisesti ja loppukäyttäjille ja organisaatiolleen lisäarvoa tuoden. (Vithayathil, 2017, s. 14)

Käyttäjien halukkuus pilvitallennuspalveluiden käyttöön heikkenee eli muutosvastarinta vahvistuu, jos he havaitsevat niissä yksityisyyden suojaan liittyviä riskejä tai että yksityisyyttä suojelevat politiikat puuttuvat. Tämä johtuu osittain siitä, että käyttäjillä voi olla vain hyvin rajallinen ymmärrys siitä miten heidän tietojaan voidaan pilvipalveluiden ylläpitäjien toimesta käsitellä ja missä niitä säilytetään. Monia käyttäjiä huolestuttaa, että heidän yksityisiä ja arvokkaita pilvipalveluihin tallentamiaan tietojaan voidaan mahdollisesti varastaa tai käyttää asiattomasti. Tällaisia väärinkäytöksiä voivat olla esimerkiksi

käyttäjien analysoiminen tai heidän tietojensa eteenpäin myyminen muille voittoa tavoitteleville tahoille. Mitä suuremman riskin käyttäjät tuntevat pilvipalveluista seuraavan, niin sitä vähemmän he niitä haluaisivat käyttää. Tämän vuoksi pilvipalveluiden tarjoajien tulee pystyä tarjoamaan mahdollisimman kattavia suojauksia tallennettavien tietojen suojaamiseksi. Esimerkkinä suojauksesta voidaan mainita vaikkapa käyttäjille lähetettävät SMS tai sähköpostihälytykset kirjautumisista, jotka tapahtuvat uusilla laitteilla ja salauksen käyttö tietoja tallennettaessa. Lisäksi pilvipalveluiden tarjoajilla kannattaa olla selkeät julistukset yksityisyydensuojasta tarjoamissaan palveluissa. (Yang & Li, 2015, s. 9)

Henkilöiden halukkuutta pilvipalveluiden käyttöön voidaan lisätä koulutuksella ja tarjoamalla palveluita käyttöön intranetin kautta, jolloin ne tuntuvat turvallisemmilta kuin julkisen Internetin yli käytettyinä (Arpaci, Kiliceri & Bardakci, 2014, s. 97). Mohapatran (2017, s. 1) mukaan yksityinen pilvi ja hybridipilvi koetaan turvallisemmiksi kuin muut käyttöönottomallit vaikka käyttöönottomallilla ei ole havaittavaa vaikutusta tyytyväisyyteen pilvipalvelun toimintaan. Aharonyn (2015, s. 308) mukaan tietotekniikka-alan ammattilaisten halukkuuteen pilvipalveluiden käyttöönottoon vaikuttavat heidän henkilökohtaiset ominaisuutensa ja osaamisensa tietotekniikan parissa.

2.3.3 Yhteenveto pilvipalveluiden haasteista

Yhteenvetona voidaan todeta pilvipalveluiden käyttöön liittyvän lukuisia tietoturvaan ja tietosuojaan liittyviä haasteita. Yksi haasteita aiheuttava asia on pilvipalveluiden ja niiden käytön suhteellinen uutuus, josta seuraa, että käytännöt, sopimukset, eri maiden lainsäädännöt ja asetukset voivat olla edelleen keskeneräisiä ja eri maissa erilaisia. Tallennettavan datan yksityisyys on merkittävä kysymys. Yhtäältä riskinä on luvaton pääsy järjestelmiin ja niihin tallennettuun dataan. Yksi merkittävimmistä riskitekijöistä ovat ns. pahantahtoiset sisäpiiriläiset eli henkilöt, joilla on luvallinen pääsy järjestelmiin ja jotka tahallaan tai vahingossa aiheuttavat tietoturvatapahtumia (Willison & Warkent, 2013, s. 1, D'Arcy, Hovav & Galletta, 2009, s. 1 ja Cram ym., 2017, s. 1).

2.4 Viranomaisten erityisvaatimukset tietojärjestelmille

Tässä luvussa käsitellään erityisvaatimuksia joita viranomaistoiminta asettaa tietojärjestelmille. Osa näistä asioista tulee toki huomioida myös muissa korkeaa tietoturvatasoa ylläpitävissä organisaatioissa. Luonnollisesti viranomaistoiminnassa pitää huomioida myös edellä luvussa 2.3 käsiteltyjä asioita. Tämän tutkimuksen tutkimuskysymyksen kannalta viranomaisten vaatimukset ovat keskeinen näkökulma pilvipalveluihin. Kansallista turvallisuutta käsittelevää lähdeaineistoa löytyy mm. USA:sta ja sitä on mahdollista myös soveltaa tähän tutkimukseen.

Tieto- ja tietoverkkoturvallisuus, hätätilanteisiin vastaaminen ja tiedon yhdistäminen ja hallinta ovat seikkoja, joihin kohdistuu vaatimuksia ja suosituksia USA:n Kotimaan turvallisuusviraston terrorisminvastaisessa toiminnassa. Tutkimukset hätätilanteiden osalta kohdistuvat IT:ssa siihen, miten IT varmistaa yhteentoimivuutta ja ylläpitää ja laajentaa kommunikointimahdollisuuksia. Lisäksi tutkimukset kohdistuvat siihen, miten IT tukee kommunikaatiota julkisuuden suuntaan ja miten se pystyy tarjoamaan tietoja päätöksentekijöille. Tiedon yhdistämisen ja hallinnan osalta tiedustelu- ja lainvalvontaviranomaisten tietojärjestelmissä tutkimuskohteina ovat datan louhinta ja yhdistäminen, kieliteknologia ja kuvien ja audiodatan prosessointi. (Chen, Wang ja Zeng, 2004, s. 330)

Suurin osa pilvipalveluita koskevasta tutkimuksesta on keskittynyt tutkimaan pilvipalveluiden käyttöä yksityisten organisaatioiden näkökulmasta. Tutkimuksia julkisten organisaatioiden pilvipalveluiden käytöstä on ollut selvästi vähemmän, vaikka julkishallinnolla on selkeitä erityispiirteitä yksityiseen sektoriin verrattuna. Julkisen sektorin erityispiirre joka vaikuttaa pilvipalveluiden toteuttamiseen ja operointiin on sirpaleinen ja monimutkainen valtionhallinnon ympäristö jossa on paljon eri virastoja, joilla on keskenään erilaisia tavoitteita ja vastakkaisia lainsäädäntöjä ja asetuksia toimintaa ohjaamassa. Lisäksi lainsäädännön muutokset voivat vaikuttaa nopeasti julkishallinnon toimintaan. Tutkimuksista on havaittavissa, että julkisen sektorin pilvipalveluiden käyttöä tutkitaan usein julkishallinnon kansalaisille suuntaamien palveluiden digitalisoinnin näkökulmasta. (Haag ym. 2014, s. 2128–2133.) Tämä näkökulma ei kaikilta osin tue tämän tutkimuksen näkökulmaa, jossa perehdytään viranomaisten käyttämiin järjestelmiin, joita ei tarjota kansalaisten käytettäviksi.

2.4.1 Yleisesti julkisen sektorin erityispiirteistä

Keskeiset eroavaisuudet yksityisten yrityksien ja julkisten organisaatioiden välillä voivat vaikuttaa siihen, että julkiset organisaatiot eivät ota uutta teknologiaa, kuten pilvipalveluita, käyttöön samoin kuin yksityiset. Toisin kuin julkiset organisaatiot yksityiset yritykset pyrkivät ensisijaisesti tekemään voit-

toa. Julkishallinnolle pilvipalvelut voivat tarjota mahdollisuutta kustannustehokkuuteen. Yksityisten yrityksien ja julkisten organisaatioiden välillä voi olla eroja myös organisaatioiden rakenteessa, kulttuurissa ja sosiaalisissa normeissa ja nämä voivat vaikuttaa siihen että yksityiset ja julkiset toimijat ottavat pilvipalveluita käyttöönsä eri tavoin ja eri syistä. (Shin, 2013, s. 195) Julkisen sektorin erityispiirre joka vaikuttaa pilvipalveluiden toteuttamiseen ja operointiin on sirpaleinen ja monimutkainen valtionhallinnon ympäristö jossa on paljon eri virastoja, joilla on keskenään erilaisia tavoitteita ja vastakkaisia lainsäädäntöjä ja asetuksia toimintaa ohjaamassa. (Haag ym. 2014, s. 2128–2133.)

Pilvipalveluiden käyttö on jo hyvin yleistä valtionhallinnon kriittisessäkin IT-infrastruktuurissa. Pilvipalveluiden käyttöön liittyy lukuisia riskejä jotka koskevat pilvipalveluiden toteutusta, hallinnointia ja käyttöä. Riskejä ovat muun muassa luvaton pääsy järjestelmiin ja toisaalta se, että joissain tilanteissa järjestelmät eivät ole lainkaan käytettävissä. Viranomaisten kyky hallita näitä riskejä on avaintekijä pilvipalveluiden menestykselle viranomaiskäytössä. Riskienhallinnan täytyy kulkea käsi kädessä uuden teknologian käytön kanssa jotta vältetään viranomaistoiminnan näkökulmasta ei-toivotut teknologiaan ja tiedonhallintaan kohdistuvat seuraukset. (Paquette ym., 2010, s. 245)

Monissa maissa on yksityisyydensuojaa koskevia lakeja, jotka asettavat vaatimuksia siitä, millaisen yksityisyydensuojalainsäädännön täytyy koskea niitä maita ja yrityksiä, joihin kotimaiset yritykset jakavat tietojaan pilvipalveluiden kautta. Tällaista lainsäädäntöä noudattamalla yritykset voivat saavuttaa etua käyttämällä pilvipalveluita tehostaakseen toimintaansa ja vähentääkseen toimintakulujaan. Lainsäädäntö voi suojella yrityksen asiakkaiden lisäksi myös sen työntekijöitä ja liikesalaisuuksia. Tällaiset lait ovat poliisitoiminnan kannalta oleellisia tämän tutkimuksen tekijän mielestä siksi, että jos jokin yksityinen yritys kehittää ja ylläpitää poliisin tietojärjestelmiä, niin on mahdollista, että tämän yrityksen Suomessa toimiva yksikkö osittaa osan työstä joihinkin muihin maihin. Toimimalla lainsäädännön mukaan yritys voi parantaa mainettaan sekä sisäisesti (esim. työntekijät ja hallituksen jäsenet) että ulkoisesti (asiakkaat, lainsäätäjät ja media). (Pelteret & Ophoff, 2016, s. 292.) Vaikka monet yksityistä liiketoimintaa koskevat asiat eivät suoraan vaikutakaan poliisitoimintaan, niin maineenhallinta on yksi keskeinen yhteinen asia. Esimerkiksi poliisin toimivaltuuksia säädettäessä hyvä maine jo olemassa olevan lainsäädännön noudattamisessa on tärkeää.

Julkisten organisaatioiden tietojärjestelmien siirtämistä lähitulevaisuudessa pilvipalveluihin tulee harkita arvon ja valmiuden näkökulmien perusteella. Arvo käsittää pilvipalveluiden tarjoamat hyödyt (tehokkuus, ketteryys ja innovaatioiden tukeminen) ja valmiusnäkökulma taasen sen, onko IT valmis pilvipalveluihin siirrettäväksi. Tähän vaikuttavia tekijöitä ovat tietoturva- ja tietosuojavaatimukset, palvelun ja markkinoiden ominaisuudet, hallinnon valmius ja tietojärjestelmien elinkaaren vaihe. On tarkasteltava, onko kaupallinen tai

valtionhallinnon oma palveluntarjoaja kykenevä toimittamaan halutunlaisen pilvipalvelun. USA:n hallituksen IT ohjelmilla on laajat tietoturvavaatimukset. FISMA:n (Federal Information Security Management Act) vaatimukset sisältävät muun muassa FIPS:n (Federal Information Processing Standard) noudattamisen, haavoittuvuuksien ja tietoturvatapahtumien seuraamisen, logituksen ja raportoinnin. (Kundra, 2011, s. 12–13)

Virastot ovat velvollisia varmistamaan, että niiden käyttöönottamissa pilvipalveluissa tietojärjestelmät toteutetaan tietoturvallisesti. Viraston tietoturvallisuusvaatimuksia tulee Kundran (Kundra, 2011, s. 13–14) mukaan tarkistella muun muassa seuraavilta osin:

- Lainsäädännön ja muiden säännöksien asettamat vaatimukset.
- Yksityisyyden ja luottamuksellisuuden suojaaminen tahallista väärinkäyttöä ja tahattomia virheitä ja vikoja vastaan.
- Datan eheys.
- Datan fyysinen säilytyspaikka ja keillä kaikilla on sinne pääsy.
- Hallintatavat joilla varmistetaan pilvipalvelutarjoajan riittävä läpinäkyvyys, turvallisuus ja hallinnolliset kontrollit sekä kyky antaa virastolle informaatiota, jonka avulla se voi asianmukaisesti ja itsenäisesti valvoa näitä kontrollimekanismeja.

Viranomaisen siirtyessä pilvipalvelun käyttöön sen täytyy varmistua tietoturvallisuudesta ja siitä että dataa hallinnoidaan asianmukaisesti, jotta ei vaaranneta kansalaisten yksityisyyttä ja kansallista turvallisuutta. Pilvipalveluihin siirtyminen edellyttää riskienhallintaa eli riskien arvioimista ja toimenpiteitä niiden pienentämiseksi hyväksyttävälle tasolle. Tietoturvakontrollit tulee tasapainottaa suhteessa pilvipalveluiden muodostamiin riskeihin siten, että kustannukset eivät nouse liian korkeiksi ja ettei aiheuteta liikaa tehottomuutta. (Kundra, 2011, s. 26)

Julkisissa organisaatioissa poliittiset ja lainsäädännöstä johtuvat asiat voivat vaikuttaa paljon tiedonjakamista parantavissa tietojärjestelmäprojekteissa. Esteet voivat olla teknisiä, organisatoorisia, poliittisia tai lainsäädännöstä johtuvia ja ne voivat estää saavuttamasta projektien tavoitteita ja mahdollisia hyötyjä. Poliittiset periaatteet voivat luoda esteitä koska niillä voidaan nähdä olevan suurempi arvo kuin mitä projektilla mahdollisesti saavutettavilla hyödyillä olisi. Projektin toteuttaminen voi myös tarvita lainsäädännöllistä tukea, joka lähtökohtaisesti mahdollistaa projektin toteuttamisen ja jonka puuttuminen voi mahdollisesti estää projektin kokonaan tai osittain. (Gil-Garcia ym., 2007, s. 123)

Sähköisen hallinnon projekteihin voi osallistua lukuisia julkishallinnon organisaatioita, yrityksiä ja myös voittoa tavoittelemattomia organisaatioita joiden tarkoituksena on jakaa dataa keskenään ja mahdollisesti myös integroida joitain liiketoimintaprosessejaan. Tällaisten projektien aloittamiseksi tarvitaan odotuksia projekteilla saavutettavista eduista. Organisaatioiden johdon tulee huomioida, että käsitykset saavutettavista eduista ja projektin esteistä voivat olla erilaisia yksityisellä ja julkisella puolella. (Gil-Garcia ym., 2007, s. 131)

2.4.2 Käyttäjien valvonta ja kontrollointi

Viranomaisten tietojärjestelmissä käsiteltävien tietojen oikeellisuus ja tietojen asianmukainen käsittely ovat keskeisiä asioita ihmisten tietosuojan, lainsäädännön vaatimuksien että viranomaisten julkisuuskuvankin takia. Suomessa on ollut useita tapauksia, joissa jopa kymmenet poliisit ovat saaneet tuomioita heidän tarkasteltuaan työhönsä liittymättömästi rikosrekisteritietoja. Tämän takia käyttäjien valvonta ja kontrollointi ovat keskeinen viranomaistoimintaan kuuluvana vaatimuksena, vaikka toki muillakin toimialoilla asia on huomioitava.

Muodollisen ja epämuodollisen kontrollin ja työntekijöiden tietoturvapolitiikkojen rikkomisaikomuksien väliset vuorovaikutussuhteet organisaatioissa ovat sellaisia, että tietoturvapolitiikan rikkomisesta aiheutuvat riittävän vakavat seuraamukset ehkäisevät tietoturvarikkomuksia. Tietoturvapolitiikan vastaisista teoista kiinnijäämisen todennäköisyydellä sen sijaan ei ole mainittavaa ennaltaehkäisevää vaikutusta. Työntekijän kiinnittyneisyydellä lähiesimieheensä ja työtovereihinsa ei ole vaikutusta työntekijän mahdollisiin aikomuksiin toimia tietoturvapolitiikan vastaisesti. Sen sijaan kiinnittyneisyys organisaatioon ja työhön ovat merkittäviä. Neljä vastuullistammisen mekanismia, jotka merkittävästi vähentävät käyttöoikeuksien rikkomisen aikomuksia ovat: Tunnistettavuus, tietoisuus lokien keräämisestä, tietoisuus auditoinneista ja toisten käyttäjien digitaalinen läsnäolo. (Cheng, Li, Li, Holm & Zhai, 2013, s. 454–455.) Vancen ja muiden (2014, s. 23) mukaan käyttäjien pitää havaita olevansa vastuussa siitä, miten he käyttävät käyttöoikeuksiaan tietojärjestelmissä.

Vähimpien käyttöoikeuksien periaate on yksi yleisesti käytetty ratkaisu käyttöoikeuksien rikkomisen ongelmaan ja se sopii hyvin käytettäväksi myös poliisin tietojärjestelmissä. Sitä noudatettaessa kullakin käyttäjällä on oikeudet tehdä vain niitä asioita, joita hänen tarvitsee työssään tehdä. Vaikka tämä periaate onkin järkevä, niin se myös aiheuttaa organisaatioille useita ongelmia. Ensinnäkään periaate ei estä väärinkäyttämästä käyttöoikeuksia, jotka sen puitteissa myönnetään. Toisekseen organisaatioiden jatkuva muuttumisen ja dynaamisuuden vuoksi on vaikeaa ylläpitää työntekijöillä vain vähimpiä mahdollisia käyttöoikeuksia työnsä hoitamiseen. Näistä syistä johtuen organisaatiot yleensä antavat työntekijöilleen enemmän oikeuksia kuin vähimpien käyttöoikeuksien periaatteen mukaan. (Vance ym., 2014, s. 2–3)

2.4.3 Käyttövarmuus

Turvallisuusratkaisut kriittisen infrastruktuuriin suojaamisessa voidaan jakaa kahteen päätyyppiin eli omaisuuden suojaamiseen ja systeemien resilienssiin eli käyttövarmuuteen. Yhdeltä näkökulmalta käyttövarmuus on järjestelmän omaa toimintakykyä ja toipumista vikatilanteista ja toinen näkökulma on se, että kriittisen infrastruktuurin ja niihin liittyvien tietojärjestelmien toiminta on kriittistä myös muiden systeemien toiminnalle. (Haimes, Crowther & Horowitz, 2008, s. 288–291)

Omaisuuden suojaaminen on riskienhallinnan osa, jolla on tavoitteena pienentää systeemien osien haavoittuvuuksia. Systeemien käyttövarmuuden parantaminen taas tarkoittaa niitä riskienhallinnan toimia, jotka nousevat esille systeemin rakenteeseen kohdistuvista muutoksista ja rakenteen ominaisuuksista. Käyttövarmuus eli resilienssi tarkoittaa järjestelmän kykyä vastustaa merkittäviä häiriöitä ja toipua niistä hyväksyttävässä ajassa hyväksyttävin kustannuksin. Käyttövarmuutta tukevat systeemin kestävyys ja redundanssi, joka tarkoittaa systeemin jonkin komponentin vikatilanteessa systeemin muiden osien kykyä hoitaa vikaantuneen osan tehtäviä niin että systeemin toiminta ei häiriinny. Tietojärjestelmissä laitteistojen redundanssia voidaan toteuttaa kahdentamalla laitteita, esimerkiksi virtalähteitä. Informaation redundanssia voidaan parantaa varmuuskopioinneilla ja peilauksilla. Tietojärjestelmien ja fyysisen infrastruktuurin redundanssin parantaminen nostaa monesti kustannuksia ja täysin redundanssin järjestelmän rakentaminen ei ole yleensä budjettisyistä mahdollista. Tietojärjestelmän redundanssin rakentaminen voidaan mallintaa rajoitettuna optimointiongelmana. Tietojärjestelmien ja fyysisen infrastruktuurin kestävyyden parantamista esimerkiksi luonnonkatastrofeja ja terrori-iskuja vastaan tehdään parantamalla suunnittelua. (Haimes ym., 2008, s. 288–291)

2.4.4 Yhteenveto viranomaisten vaatimuksista pilvipalveluille

Viranomaiskäytön pilvipalveluille asettamista erityisistä vaatimuksista vaikuttaa olevan melko vähän akateemista tutkimusta. Tämä johtunee osaltaan siitä, että monin osin vaatimukset ovat samankaltaisia kuin yksityistenkin organisaatioiden tapauksessa. Viranomaistoiminnassa keskeisiä näkökulmia ovat lainsäädäntö, tietosuoja ja kriittisen infrastruktuurin tietojärjestelmien käyttövarmuuden turvaaminen.

Julkishallinnolle pilvipalvelut voivat tarjota mahdollisuutta kustannustehokkuuteen. Yksityisten yrityksien ja julkisten organisaatioiden välillä voi olla eroja organisaatioiden rakenteessa, kulttuurissa ja sosiaalisissa normeissa ja nämä voivat vaikuttaa siihen että yksityiset ja julkiset toimijat ottavat pilvipalveluita käyttöönsä eri tavoin ja eri syistä. (Shin, 2013, s. 195)

Julkisissa organisaatioissa poliittiset ja lainsäädännöstä johtuvat asiat voivat vaikuttaa paljon tiedonjakamista parantavissa tietojärjestelmäprojekteissa kuten pilvipalveluita käytettäessä. Esteet voivat olla teknisiä, organisatoorisia, poliittisia tai lainsäädännöstä johtuvia ja ne voivat estää saavuttamasta projektien tavoitteita ja mahdollisia hyötyjä. (Gil-Garcia ym., 2007, s. 123)

Viranomaisten kyky hallita riskejä on avaintekijä pilvipalveluiden menestykselle viranomaiskäytössä. Riskienhallinnan täytyy kulkea käsi kädessä uuden teknologian käytön kanssa jotta vältetään viranomaistoiminnan näkökulmasta ei-toivotut teknologiaan ja tiedonhallintaan kohdistuvat seuraukset. (Paquette ym., 2010, s. 245)

2.5 Yhteenveto teoriakirjallisuuskatsauksesta

Edellä luvuissa 2.1 – 2.4 on käsitelty pilvipalveluiden määritelmiä, etuja ja haasteita sekä viranomaisten erityisvaatimuksia tietojärjestelmille. Aiheesta on koottu perustiedot, jotka osaltaan mahdollistavat empiirisen tutkimuksen suunnittelun ja toteuttamisen. Tässä luvussa kootaan yhteenveto näistä asioista.

Kokonaisuutena voidaan perustellusti sanoa pilvipalveluiden käytön tarjoavan runsaasti erilaisia etuja käyttäjilleen. Monet näistä eduista syntyvät pilvipalveluiden tarjoajien hyödyntäessä suuruuden ekonomiaa (Vithayathil, 2017, s. 6), infrastruktuurin keskittämistä ja virtualisointia. Pilvipalveluiden avulla mahdollisesti saavutettavissa olevia etuja ovat muun muassa halvempi hinta, joustavuus, päivityksien jakelun helpottuminen, laiteresurssien jakaminen ja tehokkaampi käyttö, resilienssin paraneminen, riskien siirtäminen, tietojen jaettavuus ja saavutettavuus, tietoturvan mahdollinen paraneminen tietyiltä osin ja järjestelmien yhteentoimivuus. Pilvipalvelut nopeuttavat ja helpottavat erityisesti pienten tietojärjestelmien toteuttamista, kun ne voidaan toteuttaa suoraan olemassa olevaan pilveen ilman laitehankintoja yms. (Jones, 2015, s. 4.) Datan keskitetty tallentaminen helpottaa sen varmuuskopiointia ja hallintaa. Virtualisointi voi vähentää tarvittavien palvelimien määrää ja tämä pienentää tarvittavaa fyysistä tilaa ja järjestelmien energiantarvetta (Li ym., 2015, s. 1). Pilvipalveluiden tarjoamat edut voidaan jaotella strategiselle, taktiselle ja operationaaliselle tasolle (Jones ym., 2017, s. 5). Etujen ja käyttöönottoa tukevien syiden lisäksi tulee kuitenkin tarkastella myös pilvipalveluihin liittyviä haasteita.

Tietoturvaan ja -suojaan liittyy lukuisia haasteita joita tulee huomioida pilvipalveluissa. Yksi näistä on pilvipalveluiden ja niiden käytön suhteellinen uutuus, josta seuraa, että käytännöt, sopimukset, eri maiden lainsäädännöt ja asetukset voivat olla edelleen keskeneräisiä ja eri maissa erilaisia. Tallennettavan datan yksityisyys on merkittävä kysymys. Yhtäältä riskinä on luvaton pääsy järjestelmiin ja niihin tallennettuun dataan. Yksi merkittävimmistä riskitekijöistä ovat ns. pahantahtoiset sisäpiiriläiset eli henkilöt, joilla on luvallinen pää-

sy järjestelmiin ja jotka tahallaan tai vahingossa aiheuttavat tietoturvatapahtumia (Willison & Warkent, 2013, s. 1, D'Arcy, Hovav & Galletta, 2009, s. 1 ja Cram ym., 2017, s. 1).

Viranomaiskäytön pilvipalveluille asettamista erityisistä vaatimuksista vaikuttaa olevan melko vähän akateemista tutkimusta sellaisissa tilanteissa, joissa pilvipalveluna toteutettava tietojärjestelmä on tarkoitettu viranomaisen omaan käyttöön eikä kansalaisille tarjottavien sähköisten palveluiden alustaksi. Tämä johtunee osaltaan siitä, että monin osin vaatimukset ovat samankaltaisia kuin yksityistenkin organisaatioiden tapauksessa. Viranomaistoiminnassa keskeisiä näkökulmia ovat lainsäädäntö, tietosuoja ja kriittisen infrastruktuurin tietojärjestelmien käyttövarmuuden turvaaminen.

Julkisen sektorin erityispiirre joka vaikuttaa pilvipalveluiden toteuttamiseen ja operointiin on sirpaleinen ja monimutkainen valtionhallinnon ympäristö jossa on paljon eri virastoja, joilla on keskenään erilaisia tavoitteita ja vastakkaisia lainsäädäntöjä ja asetuksia toimintaa ohjaamassa. (Haag ym. 2014, s. 2128–2133.) Julkishallinnolle pilvipalvelut voivat tarjota mahdollisuutta kustannustehokkuuteen. Yksityisten yrityksien ja julkisten organisaatioiden välillä voi olla eroja organisaatioiden rakenteessa, kulttuurissa ja sosiaalisissa normeissa ja nämä voivat vaikuttaa siihen että yksityiset ja julkiset toimijat ottavat pilvipalveluita käyttöönsä eri tavoin ja eri syistä. (Shin, 2013, s. 195)

Julkisissa organisaatioissa poliittiset ja lainsäädännöstä johtuvat asiat voivat vaikuttaa tiedonjakamista parantavissa tietojärjestelmäprojekteissa kuten pilvipalveluita käytettäessä. Esteet voivat olla teknisiä, organisatoorisia, poliittisia tai lainsäädännöllisiä ja ne voivat estää saavuttamasta projektien tavoitteita ja mahdollisia hyötyjä. (Gil-Garcia ym., 2007, s. 123) Viranomaisten kyky hallita riskejä on avaintekijä pilvipalveluiden menestykselle viranomaiskäytössä. Riskienhallinnan täytyy kulkea käsi kädessä uuden teknologian käytön kanssa jotta vältetään viranomaistoiminnan näkökulmasta ei-toivotut teknologiaan ja tiedonhallintaan kohdistuvat seuraukset. (Paquette ym., 2010, s. 245)

Teoriakirjallisuuden pohjalta pilvipalveluista ja viranomaisten tietojärjestelmiin kohdistamista vaatimuksista on koossa paljon tietoja. Nämä eivät kuitenkaan vastaa tämän tutkimuksen tutkimuskysymykseen, joten Suomen ja nimenomaan suomen poliisihallinnonalan osalta tarvitaan kuitenkin lisätietoja. Eli onko poliisihallinnossa missä määrin käytetty pilvipalveluita ja miten niihin liittyviä lakeja, ohjeistuksia yms. tulkitaan ja sovelletaan. Seuraavissa luvuissa tarkastellaan tutkimuskysymykseen vastaamiseksi käytäntöä kahdella eri tutkimusmenetelmällä eli kirjallisen aineiston läpikäynnillä ja haastatteluilla. Ensin esitellään käytetyt tutkimusmenetelmät ja sitten käsitellään suomalaista lainsäädäntöä ja valtionhallinnon ohjeistuksia niiltä osin mitkä vaikuttavat poliisihallinnonalan tietojärjestelmiin ja pilvipalveluiden käyttömahdollisuuksiin. Sen jälkeen käsitellään haastattelututkimuksella saatuja tuloksia.

3 TUTKIMUSMENETELMÄT

Tässä luvussa esitellään tutkimuksessa käytetyt tutkimusmenetelmät ja perustellaan niiden valintaa ja käyttöä. Haastatelluista asiantuntijoista kerrotaan taustatietoja ja haastattelujen rakenne ja haastatteluaineistojen analysointi kuvataan. Lisäksi esitellään kirjallisen aineiston valinta ja läpikäynti.

3.1 Tutkimusmenetelmät ja niiden valinta

Tämä tutkimus toteutettiin laadullisena tutkimuksena. Laadullinen tutkimus soveltuu käytettäväksi hyvin silloin, kun ollaan kiinnostuneita yksityiskohtaisista rakenteista ja yksittäisten toimijoiden merkitysrakenteista ja halutaan tutkia asioita, joita ei voida tutkia koejärjestelyillä (Metsämuuronen, 2011, s. 220). Aineiston hankinnassa on mahdollista käyttää yhtä tai useampaa metodia (Metsämuuronen, 2011, s. 244) ja tähän tutkimukseen metodeiksi valittiin kirjallisen materiaalin käyttö ja puolistrukturoidut haastattelut. Puolistrukturoidut haastattelut sopivat hyvin tutkimuksiin, joissa haastateltava ryhmä ei ole yhtenäinen ja joissa selvitetään heikosti tiedostettuja asioita (Metsämuuronen, 2011, s. 247) ja joissa halutaan mahdollisuus vastauksien täsmentämiseen (Metsämuuronen, 2011, s. 245). Haastattelujen käyttöä tuki myös se, että ne ovat yksi tärkeimmistä tiedonkeruutavoista laadullisessa tutkimuksessa (Myers & Newman, 2007, s. 2).

Lainsäädäntöön ja ohjeistuksiin yms. perehtymiseksi oli välttämätöntä ensin valita jollain rajauksilla mihin aineistoihin perehdytään ja sitten lukea valitut materiaalit. Se miten asiantuntijat kirjallista materiaalia tulkitsevat ja työssään soveltavat, selviää kysymällä näiltä asiantuntijoilta. Asiantuntijoilta saatiin myös tietoa, mitkä lait yms. heidän mielestään ovat relevantteja, joten haastattelut tukivat myös kirjallisen materiaalin valintaa. Tutkimuksessa oli mielekästä käyttää näitä molempia menetelmiä, koska yhdessä ne mahdollistivat perehtymisen sekä siihen mitä lainsäädännössä, ohjeistuksissa yms. sanotaan että sii-

hen, miten materiaaleja tulkitaan ja sovelletaan. Kummankaan käyttö yksinään ei olisi antanut kokonaiskuvaa tutkimuskysymykseen vastaamiseksi.

Yksi oleellinen syy puolistrukturoitujen haastattelujen käyttämiseen aineistonkeruumenetelmänä oli se, että näin asiantuntijoilta oli mahdollista saada tietoa sellaisistakin asioista, joita ei haastattelurunkoa kirjoitettaessa tiedetty nousevan haastatteluissa esille. Tutkimuksen aikana oli tarkoituksenmukaista voida tarpeen mukaan huomioida asiantuntijoilta saatuja vastauksia siinä, mitä tulevissa haastatteluissa jatkossa kysyttäisiin. Lisäksi tutkimusta suunniteltaessa oli nähtävissä, että mahdollisia haastateltavia asiantuntijoita ei ole kovinkaan suurta joukkoa, joten kvantitatiivinen tutkimus ei olisi ollut mielekäs, koska otos olisi jäänyt hyvin pieneksi.

Haastateltuja oli yhteensä seitsemän henkilöä. Heille luvattiin anonymiteetti haastatteluissa, joten heistä ei kerrota tietoja joiden avulla heidät olisi mahdollista tunnistaa. Osa heistä on poliisihallinnonalan työntekijöitä eri organisaatioista ja loput olivat Viestintävirastolta ja eräältä viranomaisten tietojärjestelmien auditointeja tekevältä yritykseltä. Haastateltavissa oli yksi tai useampia seuraavilla nimikkeillä: auditoija, juristi, järjestelmäasiantuntija, projektipäällikkö ja tietoturva-asiantuntija. Mahdollisten haastateltavien asiantuntijoiden joukko oli rajallinen, joten oli tärkeää saada riittävän moni suostumaan haastateltaviksi. Muutamat haastateltaviksi kysytyt asiantuntijat kieltäytyivät pääasiassa ajanpuutteeseen vedoten. Haastateltaville kerrottiin, että pro gradu tulee olemaan julkinen, joten heidän ei tule kertoa mitään salassa pidettäviä tietoja.

Empiirisessä tutkimuksessa käytetty kirjallinen aineisto on pääsääntöisesti julkisista lähteistä saatavaa aineistoa. Se on kerätty mm. Finlexista ja VAHTI-ohje –sivustolta ja pieni osa aineistosta on POHA:n dokumentteja, jotka eivät ole julkisesti saatavilla. Keräämiseen liittyi epävarmuutta, että mitä kaikkia aineistoja tulisi huomioida. Aineiston valintaan saatiin varmuutta kysymällä haastateltavilta, mitkä ovat oleellisimmat asiaankuuluvat ohjeistukset, säädökset yms. aihepiiriin liittyen ja valitsemalla ne, jotka nousivat vastauksissa eniten esille. Aineisto rajautui vielä sitä läpikäytäessä silloin kun osoittautui, että jossain ohjeessa tai laissa ei olekaan mitään tietoa, joka auttaisi vastaamaan tutkimuskysymykseen. Aihepiiriä käsitteleviin kansainvälisiin standardeihin perehtyminen rajattiin kirjallisuuskatsauksesta pois kahdesta syystä. Ensinnäkin siksi, että ne on jo todennäköisesti huomioitu suomalaisissa säädöksissä ja ohjeistuksissa tai ne ainakin olisi ollut syytä huomioida. Toisena syynä poisrajaamiseen oli se, että pro gradun työmäärä olisi kasvanut liian isoksi, jos ne olisi otettu mukaan aineistoon.

3.2 Haastattelututkimus

3.2.1 Haastateltavien valinta

Haastateltaviksi valittiin henkilöitä, jotka ovat työskennelleet jo pidempään tietojärjestelmien kehitysprojekteissa tai tietoturvan, tietosuojan tai juridiikan parissa poliisihallinnossa tai sen kanssa yhteistyössä toimivissa organisaatioissa. Haastateltavia valittaessa henkilöille myös kerrottiin tutkimuksen tutkimuskysymyksestä ja aihepiireistä, joista haastattelussa oli tarkoitus kysyä. Tällä tavoin henkilöille tuli mahdollisuus kieltäytyä haastattelusta, jos he eivät kokeneet olevansa asiantuntevia haastateltavia tutkimukseen. Tämä tuki sitä, että haastateltaviksi valikoitui henkilöitä joilla on asiantuntemusta tutkimuksen aihepiiriin kuuluvista asioista. Lisäksi muutamat haastateltavista löytyivät kysymällä aiemmilta haastateltavilta ehdotuksia, että keitä muita kannattaisi haastatella. Tällä haastatteluiden lopussa käytettävällä tekniikalla haastateltavat johdattavat haastattelijaa toisten haastateltavien luokse ja tämä auttaa haastattelijaa keräämään riittävästi dataa (Myers & Newman, 2007, s. 14). Lisäksi tämä osoittautui muutenkin hyväksi tekniikaksi, koska haastateltavaksi kysytyt henkilöt suostuivat yleensä hyvin, jos heitä pystyi lähestymään siten, että joku jo haastatelluista oli heitä suositellut seuraavaksi haastateltavaksi. Haastateltavien asiantuntijoiden löytäminen ja suostutteleminen mukaan tutkimukseen oli nimittäin joiltain osin haasteellista. Osallistumiseen kannustettiin sillä, että tutkimuksesta tulee olemaan hyötyä poliisihallinnonalalle. Tästä huolimatta jotkut jotka todennäköisesti olisivat olleet kiinnostavia ja hyödyllisiä haastateltavia, kieltäytyivät haastattelusta.

3.2.2 Haastattelujen rakenne ja analysointi

Haastattelurunko rakennettiin kirjallisuuskatsauksen eli luvun 2 osa-alueiden pohjalta. Haastattelukysymykset ryhmiteltiin näiden perusteella viranomaisten vaatimuksiin tietojärjestelmille ja pilvipalveluiden etuihin ja haasteisiin. Näiden puitteissa kysyttiin asioita muun muassa pilvipalveluihin, ST-luokitellun tiedon käsittelemiseen ja auditointeihin liittyen. Tarkoituksena oli saada selville asiantuntijoiden näkemyksiä ja tietotaitoa näistä aihepiireistä. Lisäksi haastattelurungon rakenteessa ja haastattelutilanteiden läpiviennin suunnittelussa huomioitiin haastattelun avaus, johdanto, avainkysymykset ja haastattelun lopettamiseen valmistautuminen, jotka ovat asiat jotka vähintään tulee haastatteluiden käsikirjoituksessa huomioida (Myers & Newman, 2007, s. 14). Haastattelurunko eli haastattelukysymykset on tämän dokumentin liitteenä 1.

Haastattelurunkoa muokattiin haastatteluissa saatujen vastauksien pohjalta muutamien haastattelujen välillä. Tämän yhtenä tavoitteena oli saada lisätietoja ja eri näkökulmia koskien joitain haastatteluvastauksissa esitettyjä asioita. Eli haettiin vahvistusta tai vastaväitteitä joillekin yksittäisissä haastatteluvasta-

uksissa esitetyille asioille. Toisena tavoitteena muokkaamisella oli kysyä tarkempia tietoja asioista, joita haastattelukysymyksissä ei alun perin ollut, mutta jotka nousivat esille haastatteluissa. Lisäksi viimeisistä haastatteluista jätettiin pois muutamia kysymyksiä, kun saturaatiopiste oli jo saavutettu joidenkin asioiden osalta.

Haastattelumuistiinpanot tehtiin haastatteluiden aikana. Lisäksi haastattelut äänitettiin, jos haastateltavat tämän sallivat. Yksi haastateltavista ei halunnut äänitallennusta. Muistiinpanojen puhtaaksikirjoitus tehtiin aina 24 tunnin kuluessa haastattelusta eli siten että asiat olivat vielä tuoreena muistissa. Puhtaaksikirjoitus tehtiin haastattelussa tehtyjen muistiinpanojen pohjalta ja tarvittaessa äänitallenteita apuna käyttäen. Yleensä laadullisessa tutkimuksessa aineiston kerääminen ja analysointi tapahtuvat ainakin osittain yhtä aikaa ja näiden välillä ei välttämättä ole selvää eroa (Metsämuuronen, 2011, s. 254). Tässäkin tutkimuksessa analysointi alkoi jossain määrin jo haastatteluiden aikana ja haastattelumuistiinpanoja puhtaaksikirjoittaessa.

Seuraavaksi haastateltavien vastaukset yhdistettiin yhteen muistiinpanodokumenttiin. Tämän jälkeen kysymys-vastaus -tyyppinen rakenne muutettiin tutkimustuloksiksi. Eli yksittäisiin kysymyksiin annettuja vastauksia analysoitiin ja pohdittiin, että mitkä asiat aineistosta nousevat esille tutkimustuloksiksi. Tällaisesta toiminnasta voidaan käyttää nimitystä abstrahointi, joka tarkoittaa tutkimusaineiston järjestämistä siten, että siitä tehdyt johtopäätökset voitiin irrottaa yksittäisistä henkilöistä ja lausumista ja siirtää yleiselle käsitteelliselle ja teoreettiselle tasolle (Metsämuuronen, 2011, s. 254). Osa tutkimustuloksista todettiin sellaisiksi, jotka eivät tuo mitään uutta tietoa, joten ne jätettiin pois tuloksista. Tämän jälkeen käsiteltävät tutkimustulokset rajattiin siten, että pidettiin mukana vain tutkimuskysymykseen liittyvät tutkimustulokset.

3.3 Kirjallisten lähteiden valinta ja läpikäynti

Tässä luvussa esitellään tutkimuksessa läpikäytyjen tekstien valinta. Eli mitä kirjallisia lähteitä valittiin läpikäytäviksi ja millä perusteilla.

3.3.1 Lait ja asetukset

Lait ja asetukset valittiin tutkimukseen tutkijan harkinnan perusteella. Osa niistä nousi esille myös haastatteluvastauksissa, mikä vahvisti käsitystä, että ainakin ne tutkimuksessa kannattaa läpikäydä. Henkilötietolaki valittiin läpikäytäväksi, koska se osaltaan toteuttaa yksityisyydensuojaa turvaavia perusoikeuksia ja sitä noudatetaan silloin, kun laki henkilötietojen käsittelystä poliisitoimesta ei toisin määrää. Henkilötietolaki nousi esille myös useissa haastatteluvastauksissa. Laki ja asetus viranomaisen toiminnan julkisuudesta liittyvät

salassa pidettäviin tietoihin. Myös nämä mainittiin useissa haastatteluvastauksissa. Laki henkilötietojen käsittelystä poliisitoimessa ohjaa nimensä mukaisesti sitä, miten henkilötietoja tulee käsitellä poliisihallinnossa. Kyseessä on keskeinen laki salassa pidettävien henkilötietojen käsittelyn ja tallentamisen osalta. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa ja Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista valittiin nimiensä perusteella. Tietoyhteiskuntakaari käsittelee sähköistä viestintää ja palveluita eri muodoissaan sekä luottamuksellisuuden ja yksityisyyden toteuttamista sähköisessä viestinnässä. Siinä on pyritty kokoamaan ja uudistamaan aiemmin hajanaisempana olleita säädöksiä. Myös tämä laki mainittiin useammassa haastatteluvastauksessa. Laki ja asetus julkisen hallinnon turvallisuusverkkotoiminnasta ovat oleellisia, koska poliisihallinto käyttää turvallisuusverkkoa (TUVE) ja koska osa poliisin tietojärjestelmistä on turvallisuusverkossa. Nämä lait lähdetietoineen on koottu oheiseen taulukkoon 1 säätämisjärjestyksessään vanhemmasta uudempaan.

TAULUKKO 1 Tutkimuksessa läpikäydyt lait ja asetukset

Nimi	**Lähde**
Henkilötietolaki (523/1999)	http://www.finlex.fi/fi/laki/alkup/2015/19990523
Laki viranomaisen toiminnan julkisuudesta (621/1999)	http://www.finlex.fi/fi/laki/ajantasa/1999/19990621
Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)	http://www.finlex.fi/fi/laki/ajantasa/1999/19991030
Laki henkilötietojen käsittelystä poliisitoimessa (761/2003)	http://www.finlex.fi/fi/laki/ajantasa/2003/20030761
Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)	http://www.finlex.fi/fi/laki/ajantasa/2010/20100681
Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)	http://www.finlex.fi/fi/laki/ajantasa/2011/20111406
Tietoyhteiskuntakaari (917/2014)	http://www.finlex.fi/fi/laki/ajantasa/2014/20140917
Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015)	http://www.finlex.fi/fi/laki/alkup/2015/20150010
Asetus julkisen hallinnon turvallisuusverkkotoiminnasta (1109/2015)	http://www.finlex.fi/fi/laki/alkup/2015/20151109

3.3.2 Poliisihallituksen (POHA) esikunnan ohjeet ja määräykset

Näistä valittiin läpikäytäviksi ne, jotka otsikoidensa ja johdantojensa mukaan käsittelevät tietoturvaa ja -suojaa ja tietojärjestelmien elinkaaren vaiheita. Ne tulee huomioida, koska tietojärjestelmän kehitys- ja ylläpitotyö tapahtuu monesti eri paikoissa kuin missä järjestelmää käytetään tai missä siihen tallennetut tiedot fyysisesti ovat. Läpikäydyt POHA:n materiaalit on listattu oheisessa taulukossa 2.

TAULUKKO 2 Tutkimuksessa läpikäydyt POHA:n määräykset ja ohjeet

Nimi	Voimaantulopäivä	Päättymispäivä	Suojaustaso
Poliisin tietojärjestelmien omistajuus ja kehittämisvastuut	1.4.2010	voimassa toistaiseksi	Julkinen
Poliisin tietojärjestelmien tietoturvavaatimukset	1.11.2011	31.10.2016 jonka jälkeen voimassaoloa jatkettu	ST IV
Käyttövaltuuksien hallinta poliisissa	5.12.2012	04.12.2017	ST IV
Poliisin tietojärjestelmien käyttö ja ylläpito	1.3.2013	28.02.2018	ST IV
Poliisin salassa pidettävien tietoaineistojen käsittely	1.9.2015	31.12.2019	Julkinen
Tietojärjestelmien käyttöönotto ja elinkaaren hallinta poliisissa	1.3.2017	31.12.2019	Julkinen
Poliisin tietoturva- ja tietosuojapolitiikka	1.12.2017	30.11.2022	Julkinen

3.3.3 VAHTI-ohjeet

VAHTI-ohjeet ovat Valtiovarainministeriön alaisen Valtionhallinnon tietoturvallisuuden johtoryhmän laatimia ohjeita valtionhallinnon tietoturvaan ja -suojaan liittyen. Useista kymmenistä VAHTI-ohjeista tutkittaviksi valikoitui kuusi ohjetta otsikoidensa ja johdantotekstiensä perusteella, joissa puhuttiin tietoturvasta, varautumisesta yms. aiheista joiden voidaan olettaa liittyvän ST -luokiteltujen tietojen käsittelyyn tai pilvipalveluihin. Hankintojen ja sovelluskehityksen ohjeet ottavat kantaa tietojärjestelmien elinkaaren alkuvaiheeseen, joten ne ovat oleellisia pohdittaessa järjestelmien kehitykselle ja ylläpidolle asetettavia vaatimuksia. Läpikäydyt VAHTI-ohjeet on listattu taulukossa 3.

TAULUKKO 3 Tutkimuksessa läpikäydyt VAHTI-ohjeet

Nimi	Lähde
VAHTI 3/2010, Sisäverkko-ohje.	https://www.vahtiohje.fi/web/guest/3/2010-sisaverkko-ohje

VAHTI 3/2011, Valtion ICT-hankintojen tieto-turvaohje.	https://www.vahtiohje.fi/web/guest/3/2011-valtion-ict-hankintojen-tietoturvaohje
VAHTI 2/2012, ICT-varautumisen vaatimukset.	https://www.vahtiohje.fi/web/guest/2/2012-ict-varautumisen-vaatimukset
VAHTI 3/2012, Teknisen ICT-ympäristön tieto-turva-ohje.	https://www.vahtiohje.fi/web/guest/3/2012-teknisen-ymparistons-tietoturvataso-ohje
VAHTI 1/2013, Sovelluskehityksen tietoturvaohje.	https://www.vahtiohje.fi/web/guest/vahti-1/2013-sovelluskehityksen-tietoturvaohje
VAHTI 2/2013, Toimitilojen tieto-turvaohje.	https://www.vahtiohje.fi/web/guest/vahti-2/2013

3.3.4 Valtionhallinnon muita ohjeita ja työkaluja

Edellä mainittujen lisäksi tutkimuksessa perehdyttiin kahteen muuhun valtionhallinnon ohjedokumenttiin. Katakri on mm. turvallisuusviranomaisille suunnattu auditointityökalu. Sitä käytetään monesti poliisihallinnon tietojärjestelmien auditointien perusteena, joten siihen perehtyminen oli tutkimuksessa välttämätöntä. Katakri määrittelee lukuisia hallintoon ja fyysiseen ympäristöön ja tietotekniseen toteutukseen liittyviä tietoturvavaatimuksia eri ST-luokituksen omaaville tietoaineistoille. Lisäksi kirjallisena aineistona käytiin läpi dokumentti nimeltään Pilvipalveluiden turvallisuus. Mitä organisaatioiden tulisi huomioida pilvipalveluja hyödynnettäessä. Kyseessä on Viestintäviraston Kyberturvallisuuskeskuksen julkaisema raportti organisaatioiden pilvipalveluiden tietoturvasta. Se on suunnattu muillekin organisaatioille kuin vain valtionhallinnolle. Tiedot näistä materiaaleista on esitetty alla olevassa taulukossa 4.

TAULUKKO 4 Muita tutkimuksesssa läpikäytyjä ohjeita ja työkaluja

Nimi	**Lähde**
Katakri 2015. Tietoturvallisuuden auditointityökalu viranomaisille.	http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf
Pilvipalveluiden tietoturva organisaatioille, VIVI	https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf

4 Tutkimustulokset

Tässä luvussa käsitellään tutkimustulokset ja aineistot mihin ne perustuvat. Ensin käydään läpi haastattelututkimuksen tulokset ja sitten kirjallisen aineiston eli lainsäädännön ja ohjeiden läpikäynnin tulokset.

4.1 Haastattelututkimus

Haastattelututkimuksessa nousi esille monia mielenkiintoisia havaintoja. Ensinnäkin ST IV luokiteltujen tietojen vieminen pilvipalveluihin voisi olla mahdollista. Toisekseen tietoja yliluokitellaan joissain tapauksissa. Lisäksi lainsäädännön ja ohjeistuksien muutokset ja niiden runsas lukumäärä vaikuttavat siihen, että pilvipalveluiden käytön mahdollisuutta ei aina tiedosteta. Nykytilanteen osalta haastateltavat olivat yksimielisiä siitä, että poliisihallinnonalan tietojärjestelmiä, joissa käsitellään ST-luokiteltua tietoa, ei ole toteutettu pilvipalveluissa.

4.1.1 ST IV luokiteltujen tietojen vieminen pilvipalveluihin on mahdollista

Haastatteluiden perusteella on todettavissa, että ST IV luokiteltuja tietoja sisältävien tietojärjestelmien vienti ainakin yksityiseen pilveen ja mahdollisesti myös hybridipilveen voisi olla mahdollista. Sitä korkeammin luokiteltujen tietojen vienti pilveen taas ei haastatteluvastauksien perusteella olisi mahdollista. Havainnot ja tutkimustulos perustuvat mm. seuraaviin haastatteluissa kerrottuihin asioihin ja niistä tehtyihin tulkintoihin, jotka on koottu taulukkoon 5.

Haastatelluista asiantuntijoista ”juristit” on mainittu monikossa, koska samalla haastattelukerralla haastateltiin kahta juristia. He vastasivat kysymyksiin osittain vuorotellen sen mukaan, kumpi oli kyseiseen aiheeseen enemmän perehtynyt ja toisaalta toistensa vastauksia tarvittaessa täydentäen.

TAULUKKO 5 Pilvipalveluiden käyttömahdollisuuksista haastatteluvastauksia

Haastateltu asiantuntija	**Kertomansa asia**	**Tulkinta**
Juristit	Lainsäädännössä mikään ei suoraan estä käyttämästä julkisia pilvipalveluita ST IV-luokitellun tiedon tallentamiseen, mutta käytännössä julkinen pilvi ei toteuta riittävää tietoturvatasoa tietoturva-asetuksen, VAHTI-ohjeiden ja Katakrin näkökulmista. Etenkään se ei toteuta riittävää tietoturvatasoa jos tallennettava data sijaitsisi esimerkiksi USA:ssa, jossa on erilaisia tiedonsaantioikeuksia.	Julkista pilveä ei tulisi käyttää ainakaan ST IV:sta korkeammalle luokiteltujen tietojen tallentamiseen.
Projektipäällikkö 1	"Pilvipalveluiden käyttöä estävät tiedon salassapitovelvoitteet ja TUVE:n [Turvallisuusverkko} speksit. Pilvipalveluihin viemistä varten pitäisi huolehtia salauksista ja suojauksesta. Pitäisi tietää missä palvelut pyörivät ja keillä kaikilla on niihin pääsy."	Pilvipalveluita voisi käyttää, jos edellytykset täyttyvät (salaus, suojaus, tieto palvelun sijainnista ja henkilöistä joilla on käyttöoikeus).
Järjestelmäasiantuntija	"ST IV-luokitellut tiedot voisivat olla pilvessä. Pilveen viemisen ei tarvitse tarkoittaa tietojen viemistä USA:aan."	ST IV luokiteltuja tietoja voi viedä pilvipalveluihin.
Projektipäällikkö 2	"Valtorilla on viranomaiskäyttöön tulossa olevaa pilvipalvelua suunnitteilla."	Pilvipalveluita on tulossa viranomaiskäyttöön.
Juristit	Yksityinen pilvi olisi ST IV luokitelluille tiedoilla suositeltavampi säilytyspaikka kuin julkinen pilvi.	ST IV luokiteltuja tietoja varten yksityinen pilvi on parempi kuin julkinen.
Auditoija	"ST III -luokiteltujen tietojen vienti pilveen voi olla heikkoa kansallisten vaatimuksien osalta."	ST III luokiteltuja tietoja ei tule viedä pilvipalveluihin.

ST IV luokiteltuja tietoja on siis mahdollista viedä ainakin yksityiseen pilveen. Ilmeisesti myös pelkästään tiettyjen viranomaisten käyttöön tarkoitettu hybridipilvi olisi mahdollinen, koska kyseessä ei olisi julkinen pilvi. Varsinkin yhdistettynä luvussa 4.1.2 käsiteltävään havaintoon tietojen yliluokittelusta kyseessä on tutkimustulos, joka voisi muuttaa tietojärjestelmien toteuttamista poliisihallinnossa siten, että pilvipalveluita käytettäisiin huomattavasti nykyistä enemmän. Tämä voisi mahdollistaa pilvipalveluiden tarjoamien etujen hyödyntämistä.

ST IV luokiteltujen tietojen ja niitä käyttävien tietojärjestelmien toteuttamismahdollisuus ainakin yksityisessä pilvipalvelussa on asia, jota poliisihallinnossa ei ole hyödynnetty tähän asti tiettävästi lainkaan. Tämä johtunee osaltaan mahdollisesti siitä, että pilvipalvelut käsitetään nimenomaan julkisen pilven

kaltaisena ratkaisuna ja siten, että tietojen vieminen pilveen merkitsee niiden viemistä ulkomaille. Yksityisen tai hybridipilven käyttömahdollisuutta ei ilmeisesti ole tiedostettu riittävän hyvin.

4.1.2 Tietoja yliluokitellaan

Kuten edellä luvussa 4.1.1. todettiin, niin haastattelujen perusteella ST IV -luokitellun tiedon vieminen pilvipalveluihin on mahdollista ja sitä korkeammalle luokitellun tiedon vieminen taas ei. Tämän vuoksi tietojen ST-luokitus on keskeinen tekijä harkittaessa, että voidaanko jokin tietty tietojärjestelmä toteuttaa pilvipalveluissa. Tietojen yliluokittelu tarkoittaa sitä, että tiedot luokitellaan korkeammalle suojaustasolle kuin mitä olisi tarpeen. Vastaavasti tietojen aliluokittelu tarkoittaa tilannetta, jossa tiedot luokitellaan alemmalle suojaustasolle kuin mikä olisi perusteltua. Tässä tutkimuksessa tietojen yliluokittelu nousi esille pääasiassa tilanteissa, joissa tieto voisi olla perustellusti tasolla ST IV, mutta se luokitellaankin tasolle ST III. Näiden tasojen välillä on merkittäviä eroja siinä millaisissa pilvipalveluissa niille luokiteltujen tietojen käsittelyä ja tallennusta voidaan toteuttaa.

Haastatteluissa ei noussut esille, että tietojen luokittelussa olisi yliluokittelua julkisten tietojen ja ST IV:n välillä. Tämä johtunee ensinnäkin siitä, että poliisin tietojärjestelmissä käsiteltävät tiedot ovat hyvin usein salassa pidettäviä ja mahdollisesti myös arkaluontoisia, joten ne ovat vähintään ST IV. Toisekseen tämä johtunee siitä, että tutkimuskysymyksessäkin kohteena ovat nimenomaan ST-luokitellut tiedot tietojärjestelmissä.

Eräs keskeinen käsite tietojen ST-luokituksista puhuttaessa on kasautumisvaikutus. Kasautumisvaikutus on tilanne, jossa tietojärjestelmässä oleva suuri määrä tietyn suojaustason tietoja muodostavat yhdessä tietovarannon, jonka katsotaan nostavan tietojärjestelmän ST-luokituksen korkeammaksi, kuin mitä se olisi yksittäisen tiedon tai pienen tietomäärän kyseessä ollessa. Esimerkiksi suuri määrä ST IV luokiteltua tietoa voi yhdistettynä muodostaa ST III tietoaineiston. Kasautumisvaikutus ei kuitenkaan Katakria käytettäessä velvoita kaikkiin ST III vaatimuksiin vaan korkeamman tason mukaista suojausta edellytetään vain fyysiseltä turvallisuudelta, sovelluskerroksen turvallisuudelta, jäljitettävyydeltä, havainnointikyvyltä ja työtehtävien eriyttämiseltä. Kasautumisvaikutuksen johdosta kohonnut ST-luokitus ei kuitenkaan edellytä hyväksyttävää yhdyskäytäväratkaisua tietovarannon ja päätelaitteiden välille, vaikka päätelaitteet olisivatkin alemmalla suojaustasolla. (Katakri, 2015, s. 32). Käytännössä kuitenkaan ei ole mitenkään itsestään selvää, että missä tilanteissa kasaantumisvaikutusta pitäisi soveltaa ja missä ei. Esimerkkinä tällaisesta epäselvästä luokittelutilanteesta ST IV ja III välillä voidaan mainita telekuunteluista tallennettavat tiedot. Todennäköisesti kasautumisvaikutus on kuitenkin yksi niistä syistä joiden takia yliluokittelua ST IV:lta ST III:lle tapahtuu.

Havainnot ja tutkimustulos tietojen yliluokittelusta perustuu mm. seuraaviin haastatteluissa kerrottuihin asioihin ja niistä tehtyihin tulkintoihin, jotka on koottu taulukkoon 6.

TAULUKKO 6 Tietojen yliluokittelusta kertovat haastatteluvastaukset

Haastateltu asiantuntija	**Kertomansa asia**	**Tulkinta**
Projektipäällikkö 2	"ST-luokituspäätöksiä tehtäessä monet päätöksentekijöistä (esim. tietoturvapuolen ihmiset) haluavat luokitella tietoaineistojen salassapidon liian korkealle."	Yliluokittelua tapahtuu ainakin jonkin verran.
Projektipäällikkö 1	"Projekteissa käydään keskusteluja siitä, onko jokin tietoaineisto ST III vai ST IV. Asiasta on päättämässä sekä tietoturvaan että lainsäädäntöön perehtyneitä ihmisiä."	Tietojen luokittelua pyritään tekemään harkitusti.
Projektipäällikkö 2	"Tulisi pohtia enemmän, onko jossain tietojärjestelmässä käsiteltävä tieto oikeasti esimerkiksi ”valtion toiminnan lamauttava tieto” ja että mikä olisi mahdollisen tietovuodon aiheuttama vahinko jonkin tietyn tiedon kyseessä ollessa."	Tietojen paljastumisen tai oikeudettoman käytön vakavuus ei ole aina oikeassa suhteessa ST-luokitukseen.
Tietoturva-asiantuntija	"Noin 2-3 vuotta sitten poliisihallinnossa tarkistettiin tietojen luokituksia. Oli huojuvuutta siinä, onko ST-luokitukset tehty yhteismitallisesti ja samalla tavalla”.	Tietojen luokittelu ei ole aina yhteismitallista.
Juristit	"Tietojen luokittelu ei ole yksiselitteistä vaan se on hankalaa, koska jokainen viranomainen ohjeistaa itse tietojen luokittelun ja koska eri ihmiset ajattelevat eri tavoin."	Tietojen luokittelua ei ole helppoa tehdä kaikkialla samalla tavoin.
Juristit	Monesti tietojen luokittelusta keskusteltaessa eri yhteyksissä tulee ilmi kokemus, että tietoja yliluokitellaan. Varovaisuusperiaatteen vuoksi yliluokittelu on yleisempää ja helpompaa kuin aliluokittelu.	Yliluokittelua tapahtuu ainakin jonkin verran.
Järjestelmä-asiantuntija	"TUVE:ssa [Turvallisuusverkko] ”kaadetaan kaikki ST III:seen” vaikka edes kasaantumisvaikutuksen huomioiden tietoja ja tietojärjestelmää ei tulisi luokitella kuin ST IV:seen."	ST III:selle luokitellaan tietoja jotka voisivat olla ST IV.

Havainnot ja tutkimustulokset tietojen yliluokittelun vaikutuksista perustuvat mm. seuraaviin haastatteluissa kerrottuihin asioihin, jotka on koottu taulukkoon 7.

TAULUKKO 7 Yliluokittelun vaikutuksista kertovat haastatteluvastaukset

Haastateltu asiantuntija	**Kertomansa asia**	**Tulkinta**
Järjestelmä-asiantuntija	"ST III:ssa on todella kovat vaatimukset havainnoinnille ja lokien säilytykselle. Liian tiukat vaatimukset voivat tehdä tietojärjestelmät todella kalliiksi, jos ne toteutetaan oikein vaatimuksien mukaisesti. Eli ST III:seen ei kannattaisi yliluokitella tietoja, jotka olisivat perustellusti ST IV."	Yliluokittelusta aiheutuu kustannuksia.
Projektipäällikkö 2	"Tietoaineistojen salassapidon luokittelu liian korkealle vaikeuttaa aineistojen käyttöä ja nostaa samalla myös tietojärjestelmien toteuttamisen kustannuksia."	Yliluokittelusta aiheutuu kustannuksia ja tietojen käyttö vaikeutuu.
Projektipäällikkö 2	"Tiukat tietoturvavaatimukset haittaavat järjestelmien käytettävyyttä."	Jos vaatimukset johtuvat yliluokittelusta, niin käytettävyys huononee tarpeettomasti.
Projektipäällikkö 2	"ST III tuo hallinnointiin käytettävyysongelmia. Ei voi esim. bootata palvelimia etänä vaan pitää käydä paikan päällä dedikoidulla työasemalla tekemässä bootti tms. toimenpide."	Tietojärjestelmän ylläpitotoimien suorittaminen etätyönä ei onnistu, kun ylläpitoa voi tehdä vain tietyiltä koneilta.
Projektipäällikkö 2	"ST IV tietoja voidaan lähettää hallinnon ulkopuolelle salattuna. ST III tietojen lähettäminen menee kuriirihommiksi."	ST III:lle luokittelu tekee tietojen lähettämisestä poliisihallinnon ulkopuolelle hitaampaa ja kalliimpaa.
Projektipäällikkö 1	"Projektien aikana pitäisi olla selvää projektipäällikölle ja teknisille henkilöille, että mille ST-tasolle tehdään. Eräässä projektissa tehtiin ensin ST IV:lle ja sitten tekninen ympäristö vaatikin ST III:sta ja tästä aiheutui myöhästymistä ja lisää kustannuksia."	Kesken projektin tapahtuva ST-luokituksen korottaminen viivästyttää projektia ja nostaa kustannuksia.

Tietoturva-asiantuntija	"Joissain tapauksissa on mahdotonta toteuttaa vaatimuksia, kun ST III -järjestelmästä ei saisi olla mitään yhteyksiä Internetiin ja käytännössä joissain yhteistyötapauksissa niitä kuitenkin pitäisi olla."	ST III:lle luokittelu voi johtaa tilanteeseen, jossa järjestelmälle vaaditaan ominaisuuksia, joita on mahdotonta toteuttaa.
Tietoturva-asiantuntija	"Liian korkeat luokitukset johtavat siihen että tietojärjestelmät tulevat kalliimmiksi ja hankalammiksi ylläpitää."	Yliluokittelusta aiheutuu kustannuksia ja ylläpidon vaikeutumista.
Järjestelmä-asiantuntija	”Kaadetaan kaikki esim. TUVE:ssa ST III:seen, vaikka edes kasaantumisvaikutuksen takia ei olisi sitä. Tästä sitten seuraa sijoittaminen suojattuun ympäristöön ja sitten ko. ympäristön vaatimukset tulevat vaatimuksiksi.”	ST III:lle luokittelu johtaa vaatimuksien lisääntymiseen.
Juristit	Tietojen yliluokittelu haittaa niiden käytettävyyttä. Vastaavasti tietojen aliluokittelu vaarantaa tietoturvaa.	Yli- ja aliluokittelu ovat molemmat omilla tavoillaan haitallisia.

Tietojen luokittelu ST IV / ST III välillä ei ole mitenkään itsestään selvää. Samassakin tietojärjestelmässä eri tiedot voivat olla käytännössä hyvin erilaisia siltä osin, että millaista vahinkoa niiden paljastumisesta aiheutuisi. Käytännön esimerkkinä voidaan ajatella vaikkapa niin sanotusta Putin-rekisteristä eli poliisin salaisesta epäiltyjen rekisteristä syntynyttä kohua. Kohussahan oli kyse siitä, että Putinin nimi oli kirjattu rekisteriin perusteettomasti jonkun yksittäisen poliisin toimesta. Keskivertokansalaisen osalta tieto, että hänet on perusteetta kirjattu rekisteriin, ei olisi todennäköisesti johtanut vastaavaan kohuun mediassa ja syytteisiin ja oikeudenkäyntiin useita poliisipäällystön jäseniä vastaan kuin mitä Putinin nimen perusteettomasta kirjaamisesta ja kirjauksen paljastumisesta seurasi.

Tietojen yliluokittelusta aiheutuu useita seurauksia. Ensinnäkin se tekee haastatteluissa saatujen tietojen mukaan tietojärjestelmien toteuttamista kalliimmaksi kuin mitä se olisi, jos tietoja ei olisi yliluokiteltu. Toisekseen se tekee tietojärjestelmien toteuttamisesta vaikeampaa. Nämä johtuvat siitä, että tietojärjestelmien fyysiseen turvallisuuteen ja tekniseen tietoturvallisuuteen kohdistuu Katakrissa hyvin eritasoisia vaatimuksia sen mukaan onko tietoaineisto ST IV vai ST III tasolla. Liitteessä 2 on listattuna Katakrin vaatimuserot ST IV ja ST III tasoille. Tietojen ST-luokitus vaikuttaa myös tietojen lähettämiseen hallinnonalan ulkopuolelle siltä osin, että voiko tietoja lähettää sähköpostitse edes salattuina vai pitääkö ne kuljettaa kuriiripostilla. Tutkimuskysymyksen kannalta yliluokittelu on kiinnostavaa myös siksi, että kuten edellä luvussa 4.1.1 esitetään, niin ST IV luokiteltuja tietoja voisi käsitellä ja säilyttää ainakin yksityisessä pilvessä toisin kuin ST III luokiteltuja tietoja.

Tietojen yliluokittelun syyt jäävät tutkimusaineiston pohjalta osittain epävarmoiksi. Lähes kaikki haastateltavat mainitsivat jossain kohden haastattelua, että tietoja yliluokitellaan herkästi. Haastateltavat arvelivat tämän johtuvan jossain määrin siitä, että epävarmassa tilanteessa valitaan mieluummin turvallisempi kuin vähemmän turvallinen vaihtoehto, jotta päätöstä tekemässä olevat ihmiset eivät joudu myöhemmin vastuuseen siitä, että olisivat aliluokitelleet tiedot. Lisäksi yliluokittelua tapahtuu siksi, että tietojärjestelmän vienti Turvallisuusverkkoon (TUVE) edellyttää haastatellun järjestelmäasiantuntijan mukaan tietojen luokittelua ST III:lle. Eli vaikka tiedot itsessään olisivat luokiteltavissa ST IV:lle, niin jos niitä käyttävä tietojärjestelmä päätetään sijoittaa TUVE:een, niin silloin tiedot luokitellaan ST III:een.

4.1.3 Lainsäädännön ja ohjeistuksien määrä ja muutokset voivat johtaa siihen ettei pilvipalveluiden käyttöönoton tiedetä olevan mahdollista

Tämä luku käsittelee lainsäädäntöä ja ohjeistuksia haastatteluvastauksien puitteissa ja luvussa 4.2 niitä käsitellään kirjallisen aineiston läpikäynnin pohjalta. Lainsäädäntö ja siihen pohjautuvat hallinnonalalla velvoittavat ohjeistukset ovat ne asiat, joiden mukaan viranomaisten, kuten poliisihallinnon, tulee toimia. Pilvipalveluiden käyttämiselle poliisin tietojärjestelmien toteuttamiseen ja salassa pidettävien tietojen säilyttämiseen on merkittävää se miten tietojärjestelmien kehityksen ja ylläpidon parissa työskentelevät työntekijät tuntevat asiaa ohjaavaa lainsäädäntöä ja ohjeistuksia. Jos he ovat epävarmoja siitä saadaanko pilvipalveluita käyttää, niin he päätyvät helposti siihen ettei niitä käytetä. Tällöin uudet tietojärjestelmät toteutetaan ilman, että niiden sijoittamista millään käyttöönottomallilla tai tasoilla toimivaan pilvipalveluun harkittaisiin.

Edellä luvussa 4.1.1 on havaittu, että pilvipalveluiden käyttö on mahdollista ainakin ST IV tietoja käsiteltäessä ja tallennettaessa. Lisäksi pilvipalveluiden käyttömahdollisuus havaitaan kirjallisista aineistoista luvussa 4.2. Kuitenkin haastattelujen perusteella syntyy kuva, että kaikki asiantuntijat eivät ole tietoisia, että lainsäädännön ja ohjeistuksien mukaan pilvipalveluiden käyttö on mahdollista tietyin edellytyksin. Tai ainakaan he eivät tarkkaan ottaen tiedä mitä aiheesta sanotaan ja että missä laeissa yms. kirjallisissa aineistoissa asiaa käsitellään.

Haastateltavilla oli erilaisia näkemyksiä siitä kuinka paljon lainsäädännön ja ohjeistuksien muutokset vaikuttavat tietojärjestelmien kehitysprojekteihin ja kuinka yllättäen tai ennakoitavasti muutokset tulevat. Parhaillaankin on tekeillä useita uudistuksia, joista yksittäiset haastateltavat tiesivät, mutta eivät kaikki. Lakien, asetuksien, määräyksien ja ohjeistuksien runsas lukumäärä vaikeuttaa niiden soveltamista ja tulkintaa, koska vaatii paljon perehtymistä sanoa varmuudella, että miten jokin asia on. Tai että onko tilanne millä tavoin muuttumassa lähiaikoina.

Lainsäädäntöä ja ohjeistuksia koskevia haastatteluvastauksia ja niistä tutkijan tekemiä tulkintoja on koottu seuraavaan taulukkoon 8:

TAULUKKO 8 Lainsäädännön ja ohjeistuksien vaikutuksia koskevia vastauksia

Haastateltu asiantuntija	**Kertomansa asia**	**Tulkinta**
Projektipäällikkö 1	"Projekteissa on paljon erinomaisen sekavia vaatimuksia, joita joko on pakko noudattaa tai joita olisi kiva noudattaa. Ne kohdistuvat tietoturvaan ja -suojaan ja niitä tulee sekä yllättäen että ns. jälkijunassa kesken kehityksen mm. POHA:lta [Poliisihallitus], silloiselta Haltikilta ja TUVE:n [Turvallisuusverkko] tietoturvayksiköstä. Eli kesken projektin tulee tietoja että mitä vaatimuksia pitäisi noudattaa tai kysymyksiä että ”Olettehan noudattaneet näitä?” koskien sellaisia vaatimuksia joista projektissa ei ole aiemmin kuultu. Ongelmallista on myös että useilta eri tahoilta tulee ohjeistuksia, jolloin on epäselvää, mitä kaikkia niistä tulisi noudattaa."	Ohjeiden koetaan tulevan ennakoimattomasti ja useilta eri tahoilta ilman että on selvää, mitä kaikkia niistä tulisi noudattaa.
Projektipäällikkö 2	"Lainsäädännön ja ohjeistuksien vaatimukset eivät muutu yllättäen. Projektit eivät kompastu tällaisiin muutoksiin, vaikka vuosia kestävien projektien aikana lainsäädäntö ja ohjeistukset voivatkin muuttua."	Lainsäädännön ja ohjeiden muutoksien ei koeta tulevan yllättäen.
Tietoturva-asiantuntija	"Viime vuosina on ollut vakaampi tilanne ja ei ole tullut paljoa uutta. Tietoturva-asetuksen tultua tuli paljon uusia vaatimuksia, mutta sen jälkeen tilanne on ollut vakaampi. Vuonna 2018 tulee kuitenkin uusia vaatimuksia huomioitaviksi."	Lainsäädäntö on muuttunut ja muuttuu jatkuvasti.
Tietoturva-asiantuntija	"Ilmeisesti tietoturvatasokäsite eli ST-luokitus on muuttumassa jossain vaiheessa."	Muutoksen ennakointi etukäteen voi olla hankalaa jos asiasta ei ole tarkempaa ennakkotietoa.
Järjestelmä-asiantuntija	”Ohjeet eivät muutu, mutta ymmärrys niistä saattaa muuttua projektin aikana. Muutoksien sijaan ongelma on, että esim. VAHTI-ohjeet eivät muutu tarpeeksi usein."	Ohjeiden tulkinta voi muuttua projektin aikana.
Juristit	Lainsäädännön muutokset eivät tule täysin yllättäen. VAHTI-ohjeet ja lainsäädäntö ovat kuitenkin muuttumassa.	Lainsäädännön muutokset tulevat mahdollisesti johtamaan myös sisäministeriön ja POHA:n ohjeiden muutoksiin.

Projektipäällikkö 1	"Aikoinaan vuosia sitten erään järjestelmän tekemistä aloittaessa oli puhetta pilvipalvelun käytöstä, mutta silloin tuli kielteinen vastaus... olisiko ollut POHA:n tietoturvapäälliköltä tai Valtorin ohjeista."	Useissa projekteissa ei ole selvitetty pilvipalveluiden käyttömahdollisuutta, koska se on kertaalleen joskus todettu mahdottomaksi.
Projektipäällikkö 1	"Kun uusia ohjeita tulee kesken kaiken, niin kustannukset nousevat ja tulee viivästymisiä."	Ohjeiden muutokset kesken projektin nostavat kustannuksia ja aiheuttavat viivästyksiä.
Projektipäällikkö 2	"Pilvipalveluiden käyttömahdollisuuksia tutkaillaan. Niiden käyttöä estävät tiedon salassapitovelvoitteet ja TUVE:een liittyvät määräykset. Salaus ja suojaus pitäisi olla hallinnassa ja pitäisi tietää missä palvelut pyörivät."	Pilvipalveluita käyttömahdollisuuksiin vaikuttavat mm. salassapitovelvoitteet ja palveluiden fyysinen sijainti.
Projektipäällikkö 1	"Uusien ohjeiden tulo kesken kaiken johtunee osittain POHA:n tietoturvapuolen henkilövaihdoksista. Aina ei myöskään tiedä keneltä pitäisi kysyäkään."	Henkilövaihdokset ovat yksi syy joka voi johtaa ohjeiden yllättävään päivittymiseen.

Poliisihallinnon tietoturvaohjeistukset eroavat yleisistä tietoturvapolitiikoista ainakin muutamien seikkojen osalta. Yksi oleellinen ero on se, että jos tietojärjestelmä päätetään toteuttaa TUVE:ssa, niin se tuo järjestelmälle jo omat vaatimuksensa. Toinen ero on se, että ei ole olemassa mitään yksittäistä ohjeistusta tai tietoturvapolitiikkaa, jonka noudattaminen varmuudella riittäisi. Poliisihallinnossa vaikuttavia ohjeistuksia on sekä koko valtionhallinto koskevia (lainsäädäntö, Katakri, VAHTI-ohjeet) että vain poliisihallintoa koskevia POHA:n ohjeistuksia. Lainsäädännön muutokset tulevat nykyään monesti EU-lainsäädännöstä ja muutokset johtavat ohjeiden päivittymiseen lainsäädäntöä vastaavaksi jollain viiveellä. Yksi ongelma saattaa olla se, että lainsäädännön muutoksista ei tiedetä laajasti etukäteen tai välttämättä edes niiden jo voimaantultua ennen kuin esim. VAHTI-ohjeet tai POHA:n ohjeet sitten päivittyvät.

Haastateltavia pyydettiin luettelemaan tärkeimmät lait, jotka liittyvät poliisihallinnon tietojärjestelmiin ja tietojenkäsittelyyn niissä. Useimmat haastateltavista mainitsivat vain yhden tai muutamia lakeja ja juristit mainitsivat eniten eri lakeja. Taulukkoon 9 on koottu lista mainituista laeista ja siitä kuinka moni kyseisen lain mainitsi.

TAULUKKO 9 Haastateltavien mainitsemat lait

Lain nimi	**Mainintojen määrä**
Hallintolaki	2
Hankintalainsäädäntö	1
Henkilötietolaki	3
Julkisuuslaki	3
Laki sähköisestä asioinnista viranomaistoiminnassa	2
Pakkokeinolaki	2
Poliisilaki	1
Tietojenkäsittely poliisitoimessa	1
Tietosuojalaki	1
Tietoturva-asetus	3
Tietoyhteiskuntakaari	3
Turvallisuusselvityslaki	2

Vastauksien jakautuminen näin monelle eri laille voi johtua useista eri syistä. Ensinnäkin kukin vastaajista tarkastelee asiaa oman työtehtävänsä näkökulmasta, mikä vaikuttaa siihen, mihin lakeihin vastaaja on mahdollisesti perehtynyt. Toisekseen vastaajien ei välttämättä ole tarvinnut lakeihin koskaan perehtyäkään, koska he voivat perustellusti olettaa ohjeistuksien olevan lainmukaisia. Joka tapauksessa vastauksien jakautuminen näin monelle eri laille on mielenkiintoista. Jos puhutaan esimerkiksi siitä miten "tietojärjestelmiä ja pilvipalveluita koskeva lainsäädäntö" vaikuttaa johonkin asiaan, niin on syytä huomata, että mitään asiantuntijoiden yhteistä jaettua käsitystä ei välttämättä ole siitä, että mistä kaikista laeista ja asetuksista on kyse.

Haastatteluissa tuli myös esille, että poliisin henkilötietolakia ollaan uudistamassa EU:n tietosuoja-asetuksen johdosta. Eräs haastatelluista pohti, että mahtaakohan lainsäädännön uudistuksesta tulla seurauksia, johon ei ole osattu vielä varautua. Tätä kirjoittaessa tilanne on se, että POHA on koonnut lausuntonsa lakiluonnoksesta ja lausunto on lähtenyt sisäministeriöön tammikuussa 2018.

Oheisessa taulukossa 10 on listattuna POHA:n ohjeita ja määräyksiä, jotka koskevat mm. tietojärjestelmien kehittämistä, ylläpitoa ja tietoturvaa. Aineisto on kerätty loppuvuodesta 2017. Taulukosta on havaittavissa, että lähes joka vuosi ainakin joku aihepiiriä käsittelevä ohje tai määräys on tullut voimaan ja että osa ohjeista on jo ehtinyt vanhentua tutkimusta tehtäessä. Jos oletetaan että jokin tietojärjestelmäprojekti olisi käynnistynyt vuoden 2017 jälkipuoliskolla, niin osa aloitushetkellä voimassa olleista ohjeista ja määräyksistä olisi jo vanhentunut tätä kirjoitettaessa.

TAULUKKO 10 POHA:n ohjeet ja määräykset

Nimi	Voimaantulopäivä	Päättymispäivä	Suojaustaso
Poliisin tietojärjestelmien omistajuus ja kehittämisvastuut	1.4.2010	voimassa toistaiseksi	Julkinen
Poliisin tietojärjestelmien tietoturvavaatimukset	1.11.2011	31.10.2016 jonka jälkeen voimassaoloa jatkettu	ST IV
Käyttövaltuuksien hallinta poliisissa	5.12.2012	04.12.2017	ST IV
Poliisin tietojärjestelmien käyttö ja ylläpito	1.3.2013	28.02.2018	ST IV
Poliisin salassa pidettävien tietoaineistojen käsittely	1.9.2015	31.12.2019	Julkinen
Tietojärjestelmien käyttöönotto ja elinkaaren hallinta poliisissa	1.3.2017	31.12.2019	Julkinen
Poliisin tietoturva- ja tietosuojapolitiikka	1.12.2017	30.11.2022	Julkinen

Yhteenvetona voidaan todeta, että muutoksia lainsäädännössä ja määräyksissä ja ohjeistuksissa tapahtuu vuosittain. Juristien näkökulmasta muutokset eivät tule niin yllättäen kuin miten ne koetaan muiden toimesta. Sinänsä lainsäädännön ja ohjeistuksien muutos itsessään voi viedä asioita parempaan suuntaan, mutta muutoksista voi aiheutua ongelmia siihen miten tietojärjestelmät saadaan kehitettyä ja ylläpidettyä lainsäädännön ja ohjeistuksien mukaisina ja miten hyvin työntekijät pysyvät perillä niiden muodostamasta kokonaisuudesta. Tämä on ollut ilmeisesti yhtenä osatekijänä johtamassa siihen, ettei pilvipalveluiden käyttömahdollisuuksia ole paljoakaan selvitetty saatikka hyödynnetty poliisihallinnossa.

4.2 Kirjallisen aineiston läpikäynti

Tutkimuksessa läpikäyty kirjallinen aineisto eli lait, asetukset ja ohjeistukset valittiin ensisijaisesti tutkijan harkinnan perusteella. Toisena valintaperusteena oli se, että jos useammat haastateltavat mainitsivat jonkin tietyn lain tms. aihepiiriin oleellisesti liittyväksi, niin kyseinen teksti läpikäytiin tutkimuksessa. Läpikäydyt aineistot on lueteltu luvussa 3.3. Tässä luvussa käsitellään vain ne aineistot ja kohdat kyseisistä aineistoista, jotka liittyvät pilvipalveluihin ja jotka ovat pohjana tutkimustuloksille.

Lainsäädännöstä, ohjeistuksista yms. nousi esille mielenkiintoisia asioita, joihin perustuen tässä luvussa esitetään kaksi tutkimustulosta. Ensinnäkin se, että ST-luokiteltujen tietojen vieminen pilvipalveluihin on mahdollista tiettyjen ehtojen täyttyessä ja toisena se, että poliisin operatiivisia tietojärjestelmiä ei voi toteuttaa Suomen ulkopuolella. Nämä tutkimustulokset pääasiassa tukevat haastattelututkimuksella saatuja tutkimustuloksia.

4.2.1 Lainsäädäntö

Lainsäädäntö käsittelee pilvipalveluihin liittyviä asioita hyvin vähän. Kirjallisen aineiston läpikäynnissä löytyivät vain seuraavat lainkohdat, jotka koskevat turvallisuusviranomaisia ja turvallisuusverkon käyttövelvoitetta.

Laki julkisen hallinnon turvallisuusverkkotoiminnasta 1. luvun 2 § määrää turvallisuusverkon käyttövelvoitteen koskevan *"sellaista valtion johtamiseen ja turvallisuuteen, maanpuolustukseen, yleiseen järjestykseen ja turvallisuuteen, rajaturvallisuuteen, pelastustoimintaan, meripelastustoimintaan, hätäkeskustoimintaan, maahanmuuttoon ja ensihoitopalveluun liittyvää viranomaisten sisäistä, välistä ja ulkoista yhteistoimintaa ja viestintää, joissa noudatetaan korkean varautumisen tai turvallisuuden vaatimuksia. Turvallisuusverkon käyttövelvoite edellyttää 2 luvussa tarkoitettujen yhteisten palvelujen sekä laitetilojen, laitteiden ja muun infrastruktuurin käyttöä."* Eli turvallisuusverkkoa ja sen infrastruktuuria tulee käyttää jos yleiseen järjestykseen ja turvallisuuteen liittyvää viranomaisten sisäistä tai välistä viestintää jossa noudatetaan korkean varautumisen tai turvallisuuden vaatimuksia.

Saman lain **1. luvun 5 §** mukaan *"Turvallisuusverkkoon välittömästi kuuluvien laitetilojen ja laitteiden on sijaittava ja palvelut on tuotettava Suomessa. Turvallisuusverkon laitetilojen, laitteiden ja palvelutuotannon hallinta ja valvonta on hoidettava Suomessa. Turvallisuusverkkoon välittömästi kuuluvia laitteita ja palveluja voidaan sijoittaa myös Suomen ulkopuolelle, jos se on toiminnallisista syistä välttämätöntä"*.

Vaikka lainsäädäntö ei puhu pilvipalveluista paljoakaan, niin niitä käsitellään useissa ohjeissa ja määräyksissä, joita käydään läpi seuraavaksi.

4.2.2 Ohjeistukset

Pilvipalveluiden käyttöä koskevia mainintoja löytyy useista ohjeistuksista. Taulukossa 11 on suoria lainauksia VAHTI 1/2013 Sovelluskehityksen tietoturvaohjeesta ja Viestintäviraston Pilvipalveluiden tietoturva organisaatioille -ohjeesta. Lainaukset ovat kohdista, joissa käsitellään pilvipalveluissa toteutettavia tietojärjestelmiä. Nämä lainaukset sisältävät sen miten ja millä tarkkuudella pilvipalveluiden käyttöä näissä dokumenteissa ohjeistetaan. Varsinkaan viestintäviraston ohjeistus ei ole ehdotonta ja yksiselitteistä vaan se on joukko suosituksia siitä, että millaisista asioista tulisi huolehtia ja mitä tulisi pohtia tietojärjestelmien pilvipalveluihin vientiä harkittaessa.

TAULUKKO 11 Pilvipalveluiden tietoturvaan kohdistuvia vaatimuksia

Lähde	**Suora lainaus lähteestä**
VAHTI 1/2013, Sovelluskehityksen tietoturvaohje, s. 28	”Yhteenvetona voidaan todeta, että pilvipalveluissa tuotettuihin sovelluksiin pätevät samat tietoturvavaatimukset kuin omaan ympäristöön tuotettuihin tai ulkoistuskumppanin ylläpidossa oleviin sovelluksiin. Normaalien vaatimusten lisäksi pilvipalveluun sijoitettavan sovelluksen suunnittelussa tulee muistaa seuraavat erityispiirteet: Missä data sijaitsee? Erityisesti tulee varmistaa siirretäänkö henkilötietoja EU-alueen ulkopuolelle. Voiko pilvipalvelussa käytettävän sovelluksen tai tallennetun datan maantieteellinen sijainti vaihtua? Miten järjestelmään tallennetun datan saa siirrettyä pilvipalvelusta oman organisaation haltuun esimerkiksi toimittajan vaihtotilanteessa? Saako pilvipalvelun tietoturvallisuudesta, kuten arkkitehtuurista ja käytetyistä sovelluskehitysmenetelmistä, riittävästi tietoa? Voidaanko pilvipalvelun tuottajaa auditoida tai voidaanko sovelluksen tekninen tietoturvallisuus testata? Kuka on vastuussa tietojen varmuuskopioinnista? Miten varmuuskopioidun datan suojauksesta varmistutaan? Miten salausavainten hallinta on toteutettu? Miten organisaation omia tietoturvallisuuteen liittyviä palveluita, kuten käyttäjätunnistusta voidaan käyttää palvelussa?

	Tarvitseeko sovelluksen kehityksessä huomioida myös muut jaetun alustan, sovelluksen tai palvelun käyttäjät? Tarvitseeko huomioida palveluntarjoajan ylläpitäjien vahvojen oikeuksien tuoma riski?”
VIVI/FICORA, Pilvipalveluiden tietoturva organisaatioille, s. 8	”Pilvipalvelun käyttäjän tuleekin varmistaa, missä hänen tallentamansa tieto sijaitsee koko sen elinkaaren aikana. Tiedon sijainnilla on vaikutusta muun muassa seuraavasti: Mitä tietoa kyseiseen palveluun saa tallettaa oman maan lakien puitteissa? Minkä maan lakia sovelletaan mahdollisissa poikkeustapauksissa? Onko jonkin maan viranomaisilla oikeus tutkia tätä tietoaineistoa?”
VIVI/FICORA, Pilvipalveluiden tietoturva organisaatioille, s. 11	”Tallennettavaan tietoon kohdistuvia tai sen aiheuttamia rajoituksia: Pilvipalveluiden käyttöä rajoittavat lähinnä sopimusehdot ja osaltaan myös lainsäädäntö. Näiden soveltuvuutta tulee arvioida kuitenkin aina tapauskohtaisesti. Pilvipalveluiden käyttöön ryhdyttäessä organisaation on hyvä varmistaa myös omat muut sopimusvelvoitteensa. Sopimukset voivat rajoittaa esimerkiksi tietojen siirtämistä ulkomaille. Jos käyttöön suunnitellun järjestelmän on toteutettava jonkin kriteeristön mukainen suojaus- tai turvallisuustaso, täytyy ensin tutkia täyttääkö käytettäväksi suunniteltu pilvipalvelu nämä vaatimukset.”

Taulukossa 12 on esitettynä osa VAHTI 3/2012, Teknisen ICT-ympäristön tietoturva-ohjeen kuvasta 22 sivulta 58. Kyseinen kuva esittää pilvipalveluiden käyttömahdollisuuksia ST-luokiteltujen tietojen käsittelyssä ja tallentamisessa. Taulukosta selviää millaiset tuotantomallit mahdollistavat minkä ST-tasojen tietojen käsittelyn ja säilyttämisen pilvipalvelussa. Eri tuotantomalleja erotellaan taulukossa 12 seuraavien ominaisuuksiensa perusteella:

- Onko tietojärjestelmän toteuttaja organisaatio itse vai valtionhallinnon palvelukeskus vai toimittaja eli ulkopuolinen palveluntarjoajayritys.

- Onko ympäristö dedikoitu vain yhdelle asiakkaalle tai onko kapasiteetti jaettu useille valtionhallinnon asiakkaille tai myös muille, tuntemattomille, asiakkaille. Eli onko kyseessä käyttöönottomalliltaan yksityinen-, yhteisö- vai julkinen pilvipalvelu.

- Toteutetaanko palvelu Suomessa.

- Voidaanko palvelun tuottamiseen osallistuvista henkilöistä tehdä turvallisuusselvitys.

TAULUKKO 12 Eri tuotantomallien mahdollistamat tietoaineistot

Eri tuotantomallien mahdollistamat tietoaineistot	**Tietovarastot ja järjestelmät**
Dedikoitu ympäristö - organisaation itse tuottama palvelu	ST I
Dedikoitu ympäristö - valtionhallinnon palvelukeskuksen tuottama käyttöpalvelu	ST I
Dedikoitu ympäristö - toimittajan ylläpitämä palvelu - palvelu toteutetaan Suomessa	ST I
Dedikoitu ympäristö -toimittajan ylläpitämä ympäristö - turvallisuusselvitetty henkilöstö	ST I
Valtionhallinnon palvelukeskuksen tuottama jaettu kapasiteetti eri valtionhallinnon asiakkaille - palvelu tuotetaan Suomessa	ST II
Toimittajan tuottama jaettu kapasiteetti usealle eri valtionhallinnon asiakkaalle - palvelu tuotetaan kokonaisuudessaan Suomessa	ST III
Toimittajan tuottama jaettu kapasiteetti usealle eri asiakkaalle (tuntemattomia) - palvelu tuotetaan kokonaisuudessaan Suomessa	ST III riskiarviointi / ST IV
Toimittajan tuottama jaettu kapasiteetti usealle eri asiakkaalle (tuntemattomia) - palvelun tuottamiseen osallistuvista henkilöistä on mahdollista tehdä turvaselvitys	ST III riskiarviointi / ST IV
Toimittajan tuottama jaettu kapasiteetti usealle eri asiakkaalle (tuntemattomia) - palvelua voidaan tuottaa mistä tahansa, palvelun tuottamiseen liittyviä henkilöitä ei ole mahdollista nimetä, organisaatio ei voi auditoida palvelua.	julkinen tieto

Taulukon 12 mukaan ST IV tietoja voi viedä ulkopuolisen toimittajan jaetulle kapasiteetille, jota tarjotaan useille tuntemattomille asiakkaille. Tämä tarkoittaa siis sitä, että tämän ohjeen mukaan tietoja voidaan viedä julkiseen pilveen. Palvelu voidaan toteuttaa kokonaisuudessaan Suomessa. Jos se toteutetaan ulkomailla, niin yhtenä edellytyksenä on, että palvelun tuottamiseen liittyvistä henkilöistä on mahdollista tehdä turvallisuusselvitykset. Taulukossa 12 esitettyjen ohjeiden mukaan on niin, että jos julkiseen pilveen tai ulkomaille viedään ST III tietoja, niin tietojen viemisestä tulee tehdä riskiarviointi. Suomessa toteutettu ulkopuolisen toimittajan tarjoamaan jaettuun resurssiin perustuva palvelu, jossa on vain valtionhallinnon asiakkaita, on määritelmällisesti yhteisöpilvi. Sellaisessa voidaan käsitellä korkeintaan ST III luokiteltua tietoa.

Taulukosta 12 on havaittavissa, että valtionhallinnon palvelukeskuksen tuottamassa pilvipalvelussa voidaan käsitellä jopa ST I luokiteltuja tietoja tämän ohjeen mukaan. Myös ulkopuolisen toimittajan tuottamissa pilvipalveluissa voidaan käsitellä jopa ST I tasolle luokiteltuja tietoja, kunhan kyseessä on dedikoitu ympäristö, joka on toteutettu kokonaan Suomessa ja jonka henkilöstö on turvaselvitettyä.

ICT-varautumisen vaatimustasoista korotetun tason osalta on määritelty VAHTI 2/2012 ohjeessa, että *"jos palvelut ja järjestelmät ovat merkityksellisiä yhteiskunnan elintärkeille toiminnoille ja poikkeusolojen toiminnalle, niin on huolehdittava niiden toimintaedellytyksistä myös tilanteissa, joissa tietoliikenneyhteydet Suomesta ulkomaille ovat lamautuneet. Näin ollen korotetun tason palvelutuottajille voidaan asettaa joitakin erityisvaatimuksia muun muassa ulkomailla tuotettaviin palveluihin ja niiden tarkastuksiin liittyen"*. (VAHTI 2/2012, s. 22). Osa poliisin operatiivisista tietojärjestelmistä on varmaankin tämän ohjeen piiriin kuuluvia ja osa ei.

Korkean vaatimustason järjestelmiä ovat VAHTI 2/2012 -ohjeen mukaan esimerkiksi hallinnon turvallisuusverkko ja turvallisuusviranomaisten operatiiviset järjestelmät. Tämä koskee siis poliisin operatiivisia järjestelmiä. Korkealle tasolle luokiteltuihin tietojärjestelmiin kohdistuva vaatimus jatkuvuudenhallinnalle on, että *"vakavissa, laajoissa häiriötilanteissa toimenpiteet tulee tehdä Suomesta ja Suomen lainsäädännön (esim. tietoliikennekatkokset ja poikkeusolojen toimivaltuudet) alaisena"* (VAHTI 2/2012, s. 76). Korkealle tasolle sijoitettavien palvelujen tulee siis toimia, vaikka tietoliikenneyhteydet ulkomaille olisivat poikki. Voidaan siis todeta, että tällaisia järjestelmiä ei voida sijoittaa Suomen ulkopuolelle.

VAHTI 3/2011, Valtion ICT-hankintojen tietoturvaohje määrittelee, että *"keskeisissä valtakunnallisissa tieto- ja viestintäjärjestelmissä yksittäisen kohteen lamautuminen tai vaurio ei saa lamauttaa koko järjestelmää. Yhteiskunnan keskeisimmät tietojärjestelmät ja tietovarannot on hajautettava maantieteellisesti kahteen paikkaan. Yhteiskunnan toimivuudelle kriittisiä tietojärjestelmiä suunniteltaessa ja rakennettaessa on varmistettava, että niihin liittyvän ohjauksen, ylläpidon, järjestelmähallinnan ja teknisen tuen osaaminen säilyy Suomessa tai ohjaus- ja hallintakyky on oltava mahdollista palauttaa Suomeen. Keskeisten sovellusten tietovarantojen tulee olla Suomessa"*. (VAHTI 3/2011, s. 21). Tämä vaatimus ei koske kaikkia poliisin operatiivisia tietojärjestelmiä, mutta varmastikin joitakin niistä.

Riskien huomioimisen osalta VAHTI 3/2011:ssa kerrotaan, että *"Uudet teknologiat ja toimintamallit tuovat mukanaan uusia uhkia, jotka tulee huomioida riskikartoituksessa. Esimerkiksi pilvipalveluita, jaettua kapasiteettia ja virtualisoituja käyttöpalveluympäristöjä käytettäessä palvelun tilaajalla ei aina ole mahdollisuutta valita missä palvelu ja siihen liittyvät tietovarannot sijaitsevat. Aidot pilvipalvelut eivät myöskään yleensä ole auditoitavissa. Kun palveluita tuotetaan Suomen ulkopuolelta, niin riskeiksi voivat muodostua esimerkiksi kansainvälisten tietoliikenneyhteyksien toimivuus tai niihin liittyvät viiveet."* (VAHTI 3/2011, s. 33) Tämä on tutkimuksen kannalta kiinnostava lainaus, koska kyseessä on yksi harvoista kohdista VAHTI -ohjeissa, joissa puhutaan nimenomaan pilvipalveluista. Tämä ohjeistus puhuu tavallaan pilvipalveluiden käyttöä vastaan, koska poliisihallinnon uudet tietojärjestelmät on auditoitava ja tässä sanotaan, että *"aidot pilvipalvelut eivät yleensä ole auditoitavissa"*. Ohje kuitenkin sallii pilvipalvelut, jos niiden tiedetään sijaitsevan Suomessa.

POHA:n ohje Poliisin tietojärjestelmien tietoturvavaatimuksista asettaa lukuisia vaatimuksia ulkomailla tehtävälle tietojärjestelmäkehitykselle ja työskentelylle poliisin tietojärjestelmien parissa. Ensinnäkin ulkomailla tietojärjestelmäkehitystä tulee tehdä vain ei-kriittisten komponenttien osalta ja vain tarkoin harkituissa tapauksissa. Toinen keskeinen vaatimus on, että ulkomainen toimittaja saa käsitellä korkeintaan ST IV luokiteltua salassa pidettävää tietoa. Eli jos tietojärjestelmän kehityksen tms. parissa työskentely edellyttää ST III luokiteltujen tietojen käsittelyä, niin tällaista työtä ei voida teettää muualla kuin Suomessa.

POHA:n määräys Poliisin salassa pidettävien tietoaineistojen käsittelystä määrittelee arkaluonteisia henkilötietoja sisältävien asiakirjojen luokituksen vähintään ST IV tasolle. Lisäksi määräyksen mukaan tietojärjestelmän tulee täyttää korotetun turvallisuustason vaatimukset, jos siinä käsitellään biometrisiä tunnisteita tai arkaluonteisia henkilötietoja. Määräys estää myös yksiselitteisesti poliisin tietojärjestelmistä tuotantodatan, henkilötietojen tai yksityiskohtaisten teknisen infrastruktuurin tietojen toimittamisen ulkomaille. Huoltoyhteydet ulkomailta sallitaan vain kehitys- ja testiympäristöihin ja niihinkin vain tarpeen vaatiessa ja valvotusti. Nämä vaatimukset estävät yksiselitteisesti poliisin tietojärjestelmien toteuttamisen niin, että niiden ylläpitoa tehtäisiin Suomen ulkopuolelta tai että niiden tietoja tallennettaisiin Suomen ulkopuolelle.

Yhteenvetona ohjeistuksista voidaan todeta, että VAHTI-ohjeet ja Viestintäviraston ohjeet eivät aseta tietojärjestelmien toteutuksella niin tiukkoja raameja kuin POHA:n ohjeet ja määräykset. Ne loppujenlopuksi määrittelevät sen, miten ja missä poliisihallinnonalan tietojärjestelmiä kehitetään ja ylläpidetään tietoturva- ja tietosuoja-asiat huomioiden.

4.2.3 Yhteenveto kirjallisesta aineistosta

Edellä läpikäydyn kirjallisen aineiston perusteella muodostuu kaksi tutkimustulosta:

- ST-luokiteltujen tietojen vieminen pilvipalveluihin on mahdollista tiettyjen ehtojen täyttyessä

- Poliisin operatiivisia tietojärjestelmiä ei voi toteuttaa Suomen ulkopuolella

Kokonaisuutena lainsäädäntö, VAHTI-ohjeet, Viestintäviraston ohjeet ja POHA:n ohjeet ja määräykset johtavat yksiselitteisesti siihen, että poliisin operatiivisia, salassa pidettävää tietoa sisältäviä tietojärjestelmiä ei voida toteuttaa Suomen ulkopuolella. POHA:n ohjeet ja määräykset asettavat tiukempia vaatimuksia kuin VAHTI-ohjeet ja Viestintäviraston ohjeet ja niiden perusteella keskeistä on tietojärjestelmien ja niissä tallennettavan tiedon sijainti. Poliisihallinnonalan tietojärjestelmiä on mahdollista toteuttaa pilvipalveluissa, kunhan tietojen tallennus ja niiden käsittely ja järjestelmien ylläpito tapahtuvat Suomessa.

5 POHDINTA

Tässä pro gradussa on koottu kirjallisuuskatsaus luvussa 2. Kirjallisuuskatsauksessa käsitellään pilvipalveluiden määritelmiä, etuja, haasteita ja viranomaisten erityisvaatimuksia tietojärjestelmille. Tämän lisäksi on toteutettu empiirinen tutkimus, jossa käytettiin menetelminä asiantuntijahaastatteluita ja kirjallisen aineiston keräämistä ja läpikäyntiä, kuten luvussa 3 on kuvattu. Empiirisen tutkimuksen tulokset on perusteltu ja esitelty luvussa 4. Tutkimustulokset ovat seuraavat:

- ST IV luokiteltujen tietojen vieminen pilvipalveluihin on mahdollista
- Tietoja yliluokitellaan
- Lainsäädännön ja ohjeistuksien määrä ja muutokset voivat johtaa siihen ettei pilvipalveluiden käyttöönoton tiedetä olevan mahdollista
- ST-luokiteltujen tietojen vieminen pilvipalveluihin on mahdollista tiettyjen ehtojen täyttyessä
- Poliisin operatiivisia tietojärjestelmiä ei voi toteuttaa Suomen ulkopuolella.

Tulokset osoittavat, että poliisihallinnonalan operatiivisten tietojärjestelmien, joissa käsitellään salassa pidettävää tietoa, toteuttaminen pilvipalveluissa on mahdollista vallitsevan lainsäädännön ja ohjeistuksien puitteissa. Tulokset eivät sinänsä rajaa edes julkisia pilvipalveluita täysin pois, jos niiden hallinnointi, kehitys ja tietojen varastointi toteutettaisiin todistettavasti vain Suomessa. Käytännössä kuitenkin yksityiset tai yhteisöpilvipalvelut vaikkapa Valtorin toteuttamina soveltuvat poliisihallinnolle parhaiten. Pilvipalveluiden eri käyttöönottomallit (julkinen, yksityinen, yhteisö- ja hybridipilvi), jotka käsiteltiin luvussa 2.1, nousivatkin jonkin verran esille mm. VAHTI-ohjeista ja muutamissa haastatteluvastauksissa. Pilvipalveluiden etuja käsiteltiin luvussa 2.2 ja pilvipalveluiden haasteita luvussa 2.3.

Tutkimustuloksia aiempaan tutkimukseen reflektoidessa voidaan todeta, että tutkimuksessa esille nousseet viranomaisten käyttämiin pilvipalveluihin kohdistuvat vaatimukset ovat samantapaisia Suomessa ja kansainvälisesti. Kuten luvussa 2.4.1. esitettiin, niin Paquetten ym. (Paquette ym., 2010, s. 245) mukaan pilvipalveluiden käyttöön liittyy lukuisia riskejä jotka koskevat niiden toteutusta, hallinnointia ja käyttöä. Merkittäviä riskejä ovat muun muassa järjestelmien luvaton käyttö ja se, että joissain tilanteissa järjestelmät eivät ole lainkaan käytettävissä. Suomessa on huomioitu näitä riskejä. Luvussa 4.2.2. on tarkasteltu VAHTI-ohjeita ja POHA:n ohjeita ja määräyksiä, joilla näiden riskien toteutumisen todennäköisyyttä pyritään pienentämään sillä, että poliisin tietojärjestelmien kehittämistä Suomen ulkopuolella rajoitetaan ja tuotantodatan ja arkaluontoisten tietojen tallentaminen Suomen ulkopuolelle kielletään. Lisäksi tietojärjestelmät edellytetään toteutettavaksi niin, että niitä on mahdollista ylläpitää, vaikka yhteydet ulkomaille katkeaisivat.

Suomalainen viranomaisten tietojärjestelmiä koskeva lainsäädäntö ja ohjeistukset käsittelevät paljolti samoja asioita kuin mitä USA:n virastojen tulee ottaa huomioon pilvipalveluiden tietoturvallisuudessa. USA:n virastojen tulee huomioida pilvipalveluiden tietoturvallisuusvaatimuksia tarkastellessaan Kundran (Kundra, 2011, s. 13 - 14) mukaan seuraavat asiat:

- Lainsäädännön ja muiden säännöksien asettamat vaatimukset.
- Yksityisyyden ja luottamuksellisuuden suojaaminen tahallista väärinkäyttöä ja tahattomia virheitä ja vikoja vastaan.
- Datan eheys.
- Datan fyysinen säilytyspaikka ja keillä kaikilla on sinne pääsy.
- Hallintatavat joilla varmistetaan pilvipalvelutarjoajan riittävä läpinäkyvyys, turvallisuus ja hallinnolliset kontrollit sekä kyky antaa virastolle informaatiota, jonka avulla se voi asianmukaisesti ja itsenäisesti valvoa näitä kontrollimekanismeja.

Lisäksi pilvipalveluiden käyttöönottoon siirryttäessä viranomaisten täytyy varmistua tietoturvasta ja datan asianmukaisesta hallinnoinnista kansalaisten yksityisyyttä vaarantamatta (Kundra, 2011, s. 26). Kirjallisuuskatsauksen luvussa 2.4.3. käsiteltiin käyttövarmuutta, joka on kirjallisuudessa oleellinen asia viranomaisten tietojärjestelmistä puhuttaessa. Käyttövarmuus nousi tutkimuksessa esille myös poliisihallinnonalalla noudatettavissa säädöksissä ja ohjeissa. Tässä tutkimuksessa esille tulleet suomalaiset viranomaisvaatimukset pilvipalveluille voidaan todeta samantyyppisiksi ja samoja aiheita käsitteleviksi kuin mitä kansainvälisestikin vaaditaan.

Tässä pro gradussa käytetään Saaranen-Kauppisen ja Puusniekan määrittelyjä reliabiliteetille (Saaranen-Kauppinen & Puusniekka, 2006 A) ja validiteetille (Saaranen-Kauppinen & Puusniekka, 2006 B), koska ne ovat tutkijalle ennestään tuttuja. Seuraavissa luvuissa pohditaan tehdyn tutkimuksen ja sen tuloksien reliabiliteettiin ja validiteettiin vaikuttavia asioita.

5.1 Reliabiliteetti

Laadullisen tutkimuksen reliabiliteettia voidaan arvioida kolmelta näkökulmalta Saaranen-Kauppisen ja Puusniekan mukaan (Saaranen-Kauppinen & Puusniekka, 2006 A). Tässä luvussa reliabiliteettia käsitellään sekä näiltä että muutamilta muilta näkökulmilta.

Erityisen metodin reliaabeliuden arvioinnissa (quixotic reliability) arvioidaan jonkin tietyn metodin luotettavuutta ja johdonmukaisuutta olosuhteisiin nähden. Metodeina tutkimuksessa olivat puolistrukturoitu haastattelututkimus ja kirjallisen aineiston läpikäynti. Haastattelututkimuksen luotettavuutta paransi se, että haastattelut äänitettiin, jolloin vastauksia on ollut mahdollista läpikäydä tarvittaessa uudestaan. Haastattelujen olosuhteet pyrittiin vakioimaan käyttämällä samaa haastattelurunkoa, vaikkakin pienin muutoksin. Kirjallisen aineiston luotettavuutta parantaa myös se, että sen tarkasteluun on tarvittaessa mahdollista palata uudelleen.

Ajallinen reliaabelius (diachronic reliability) on havaintojen ja mittaustuloksien pysyvyyttä eri aikoina. Laadullisessa tutkimuksessa ei nimittäin olla tekemisissä muuttumattomien objektien kanssa (Saaranen-Kauppinen & Puusniekka, 2006 A). Ajallinen reliaabelius on hyvä näkökulma huomioitavaksi tässä tutkimuksessa, koska kirjallisen aineiston keräämisen ja tutkimuksen tekemisen aikana yksi tutkimuksessa läpikäyty POHA:n ohje ehti jo vanhentua. Lisäksi tutkimuksen aiheita koskien on parhaillaan menossa lainsäädännön ja VAHTI-ohjeiden uudistamista. Eli jos tämä tutkimus tehtäisiin uudestaan vaikkapa vuoden tai kahden kuluttua, niin sen tulokset eivät enää voisi olla aivan samoja kuin mitä ne nyt ovat. Kirjallinen aineisto olisi joiltain osiltaan muuttunut ja muutokset olisivat todennäköisesti ja toivottavasti tulleet myös haastateltavien tietoon niin, että heiltäkin saataisiin erilaisia vastauksia.

Johdonmukaisuus tuloksissa (syncronic reliability) tarkastelee sitä, miten eri menetelmillä saadut tulokset samasta tutkimusaiheesta voivat usein poiketa toisistaan. Tällöin joudutaan tarkastelemaan sitä, miten laadullisin menetelmin saadut moninaiset tulokset tutkittavasta ilmiöstä voivat pitää paikkansa (Saaranen-Kauppinen & Puusniekka, 2006 A). Tämän tutkimuksen tuloksissa on jonkin verran eroja haastattelututkimuksella ja kirjallisen aineiston analysoinnilla saaduissa tuloksissa tarkasteltaessa sitä minkä ST-luokituksien tietoaineistoja

voitaisiin mahdollisesti pilvipalveluihin viedä. Lisäksi haastatteluvastauksissa oli eräissä aiheissa erilaisia vastauksia, jotka johtuivat todennäköisesti ainakin osittain henkilöiden erilaisista työtehtävistä ja näkökulmista. Erilaiset vastaukset olivat oletettavasti subjektiivisesti totta.

Haastateltaviksi tutkimukseen ei saatu kaikkia henkilöitä keitä olisi haluttu haastatella. Otos oli nyt riittävän suuri, mutta toki se olisi voinut olla suurempikin, jos useampi henkilö olisi suostunut haastateltaviksi. Jos osa haastateltavista olisi ollut eri henkilöitä, niin se olisi saattanut painottaa tutkimustuloksia jollain tavalla eri suuntiin. Haastateltavat olivat yksimielisiä siitä että poliisin tietojärjestelmiä ei ole vielä toteutettu pilvipalveluissa. Näin ollen heillä ei voinut olla kokemusta poliisin tietojärjestelmien käytöstä pilvipalveluissa. Osa vastaajista käsitti pilvipalvelut julkisina pilvipalveluina eivätkä välttämättä olleet tietoisia yksityisistä ja yhteisöpilvipalveluista.

Lähtökohtaisesti tutkimukseen valikoituneiden haastateltavien luotettavuutta voi pitää hyvänä jo siksikin, että kyseessä ovat asiantuntijatehtävissä työskentelevät henkilöt. Haastatteluun osallistuminen oli täysin vapaaehtoista, joten jokaisella haastateltavalla on ollut jokin motivaatio suostua haastateltavaksi. Edellä mainitut seikat (halu vastata odotuksien mukaisesti, eri työtehtävistä johtuvat erilaiset näkökulmat ja se, että haastateltaviksi ei saatu kaikkia keitä olisi haluttu) vaikuttavat kuitenkin siten, että jos tutkimus tehtäisiin uudestaan, niin tulokset voisivat olla jossain määrin erilaisia sen mukaan keitä saataisiin haastateltaviksi. Haastatteluvastauksien reliabiliteettia todennäköisesti parantaisi se, jos haastateltavia olisi enemmän.

Kirjallisuuskatsauksen tekeminen, haastattelukysymyksien laadinta, haastatteluista muistiinpanojen tekeminen sekä lainsäädäntöä yms. käsittelevän kirjallisen aineiston valinta ja läpikäynti ovat kaikki aiheita, joissa tutkijan valinnat, tulkinnat ja mielipiteet voivat vaikuttaa tutkimukseen. Näiden seikkojen vaikutusta reliabiliteettiin on pyritty vähentämään prosessin dokumentoinnilla, jolloin tutkimus voitaisiin tarvittaessa toistaa mahdollisimman samanlaisena ja jotta on nähtävissä, että mitä aineistoja on läpikäyty ja mihin tulkinnat ja tulokset perustuvat.

Lisäksi on huomattava, että lainsäädännössä ja ohjeistuksissa on paljon viittauksia toisiin lakeihin, asetuksiin, ohjeisiin ja standardeihin, joita kaikkia ei ollut mahdollista käydä pro gradun työmäärän puitteissa läpi. Poisvalinnat on tehty sillä oletuksella, että ne eivät vaikuta tutkimustulokseen, mutta aina on olemassa riski, että jotain oleellista olisi jäänyt läpikäymättä. Tämä muodostaa pienen mahdollisuuden satunnaisvirheisiin tutkimustuloksissa.

5.2 Validiteetti

Tutkimuksen validiteetti kuvaa sitä, onko tutkimus pätevä. Eli sitä, onko se tehty perusteellisesti ja ovatko sen tulokset ja niiden perusteella tehdyt päätelmät ”oikeita”. Jos tutkija näkee asioiden välisiä suhteita tai periaatteita virheellisesti tai ei näe niitä lainkaan tai kysyy vääriä kysymyksiä, niin nämä voivat johtaa virheisiin tutkimuksessa. Laadullisessa tutkimuksessa pätevyys voidaan ymmärtää myös tutkimuksen uskottavuutena tai vakuuttavuutena. (Saaranen-Kauppinen & Puusniekka, 2006 B)

Tämä tutkimus vastasi tutkimuskysymykseensä, joka oli seuraava:

Miten asiaankuuluvia lakeja, asetuksia, viranomaisohjeistuksia yms. tulkitaan ja sovelletaan pohdittaessa voidaanko jokin poliisin operatiivinen, ST-luokiteltuja tietoja sisältävä tietojärjestelmä toteuttaa pilvipalveluna jollain tietyllä pilvipalveluiden käyttöönottomallilla tai tasolla?

Tutkimuksen tekijän omat mahdolliset ennakkokäsitykset vaikuttavat myös tutkimuksen validiteettiin. Tämän tutkimuksen tutkimuskysymyksen osalta tutkijalla ei ollut ennakkokäsitystä siihen millaiseen lopputulokseen tutkimus johtaisi tai millaiseen sen toivottaisiin johtavan. Tutkijan käsitys on, että ennakkokäsitykset eivät ole vaarantaneet validiteettia, mutta tämä on toki vain tutkijan oma käsitys. Ennakkokäsityksien mahdollista vaikutusta on pyritty vähentämään myös sillä, että tutkimustuloksien muodostuminen tutkimusaineistosta on kirjoitettu auki luvussa 4.

Haastattelukysymykset luotiin teoriaosuuden eli luvun 2 kirjoittamisen jälkeen. Eli kysymykset perustuvat aihepiirin kansainvälisissä julkaisuissa käsiteltyihin asioihin. Haastatteluissa esille nousseiden asioiden perusteella muutamia kysymyksiä myös lisättiin ensimmäisten haastatteluiden jälkeen. Nämä toimintatavat tukivat sitä, että haastatteluissa kysyttiin relevantteja kysymyksiä ja että tutkimus siltäkin osin on mahdollisimman validi.

Haastateltavat pyrittiin valitsemaan siten, että haastateltavien joukko olisi monipuolinen ja että erilaiset näkökulmat tulisivat esille. Haastateltavissa oli useiden eri ammattiryhmien edustajia ja he olivat töissä useilla eri organisaatioilla. Tältä osin tutkimuksen validiteettia voidaan pitää hyvänä. Toisaalta kukin haastateltava on vastannut oman työtehtävänsä ja työnantajansa näkökulmasta, joten kaikki vastaukset ovat olleet jossain määrin subjektiivisia ja haastateltavien mahdollisia joihinkin asioihin kohdistuvia virheellisiä käsityksiä sisältäviä. Tämän vaikutusta validiteettiin ei voida täysin välttää. Suurempi otos toki vähentäisi yksittäisten vastauksien painoarvoa ja antaisi paremman kuvan siitä, mikä on haastateltavien enemmistön käsitys jostain asiasta, jos osa vastauksista on toisilleen vastakkaisia.

Haastateltaville kerrottiin, että pro gradu tulee olemaan julkinen, joten heidän ei tule kertoa mitään salassa pidettäviä tietoja. On todennäköistä, että he ovat jättäneet joitain asioita sanomatta tämän takia. Asioita on voinut jäädä sanomatta joko siksi että ne on määritelty salassa pidettäviksi tai sitten poliisihallinnonalan maineen suojelemiseksi, jos joidenkin asioiden on ajateltu sille olevan haitallisia. Validiteetin kannalta ajatellen tämä ei kuitenkaan muuttaisi tutkimustulosta, jos tutkimus tehtäisiin uudestaan samoista julkisuuslähtökohdista käsin. Poliisihallinnonalan sisäisenä ja salassa pidettävänä tutkimuksena tehtäessä validiteetti olisi tältä osin oletettavasti parempi.

Haastattelukysymyksiin on saatettu vastata stereotypisesti ja sosiaalisesti hyväksyttävästi, mikä voi vähentää vastauksien luotettavuutta. Haastatteluvastauksiin on todennäköisesti vaikuttanut se, millaista kuvaa haastateltavat ovat halunneet antaa itsestään ja osaamisestaan haastattelijalle. Haastateltaville luvattiin anonymiteetti ja yksi syy tälle oli juuri se, että he voisivat vastata huolehtimatta siitä, millaisen kuvan antavat itsestään. Toisekseen anonymiteetin tarkoitus on antaa mahdollisuus kertoa myös negatiivisia asioita.

Tutkimuksen yleistettävyys on kohtuullisen hyvä suomalaisten viranomaisten parissa. VAHTI-ohjeet ja Katakri ovat laajasti käytössä suomalaisessa viranomaiskentässä, joten niihin perustuvia havaintoja ja tutkimustuloksia voidaan yleistää muillekin hallinnonaloille kuin poliisihallintoon. Läpikäydyt lainsäädännön velvoitteet koskevat useiden eri suomalaisten turvallisuusviranomaisten toimintaa. Niihin perustuvat tulokset voidaan myös siis yleistää muuallekin kuin poliisihallintoon.

Toisaalta tutkimus on kohdistunut poliisihallinnonalaan ja tutkimuksen puitteissa on läpikäyty POHA:n ohjeita ja määräyksiä. Niitä ei voida yleistää muiden suomalaisten turvallisuusviranomaisten toimintaan, koska kullakin niistä on todennäköisesti omat vastaavat ohjeistuksensa. Lisäksi turvallisuusviranomaisia toimii useiden eri ministeriöiden alla, jotka nekin voivat tehdä omia ohjeistuksiaan ja määräyksiään. Todennäköisesti suuria eroja ei ole, mutta tätä ei voida sanoa varmuudella minkään turvallisuusviranomaisen osalta perehtymättä juuri sitä koskeviin ohjeisiin ja määräyksiin.

Tämän tutkimuksen yleistettävyydestä kansainvälisesti ei voida sanoa mitään varmaa, vaikka voidaankin olettaa EU-maiden turvallisuusviranomaisia koskevan jossain määrin samantapaiset vaatimukset ja ohjeistukset kuin suomalaisia. EU on pyrkinyt monin paikoin yhtenäistämään lainsäädäntöään ja suomalaiset tietoturvaohjeistukset perustuvat merkittävässä määrin kansainvälisesti hyväksyttyihin standardeihin, joten oletettavasti suuria eroja ei ole. Tätä ei voida kuitenkaan varmuudella sanoa perehtymättä eri maiden kansallisiin säädöksiin ja ohjeistuksiin.

6 JOHTOPÄÄTÖKSET

Tässä luvussa esitellään johtopäätöksiä ja suosituksia tämän tutkimuksen pohjalta. Lisäksi esitellään ehdotuksia jatkotutkimusaiheista. Johtopäätökset ja suositukset perustuvat teoriaan eli kirjallisuuskatsauksessa luvussa 2 esille nousseisiin asioihin ja empiriaan eli tutkimustuloksista luvussa 4 selvinneisiin asioihin.

Tutkimus ei haasta vallitsevia kansainvälisiä teorioita pilvipalveluiden määritelmistä, eduista, haasteista tai viranomaisten tietojärjestelmille asettamista vaatimuksista. Tämä johtuu osittain siitä, että poliisihallinnonalalla ei nykyisellään käytetä pilvipalveluita salassa pidettävien tietojen käsittelyssä ja tallentamisessa. Tästä johtuen tutkimuksen haastatteluosuus ei voinutkaan tuoda uutta tietoa pilvipalveluista eikä tutkimuksen tuloksia siltä osin siis voida verrata aiempiin kansainvälisiin tutkimuksiin. Tutkimuksessa esille nousset vaatimukset viranomaisten tietojärjestelmille ja pilvipalveluiden käyttöön liittyvät huolenaiheet ovat kuitenkin varsin samanlaisia kuin kansainvälisestikin. Näitä vaatimuksia on käsitelty luvussa 2.4 jossa on tarkasteltu muun muassa viranomaisten riskienhallintakykyyn kohdistuvia vaatimuksia (Paquette ym., 2010, s. 245) ja tietojärjestelmien tietosuojaan kohdistuvia vaatimuksia (Kundra, 2011, s. 13–14).

Tutkimus kuitenkin kyseenalaistaa poliisihallinnonalalla vallitsevan käsityksen, että pilvipalveluita ei voitaisi lainkaan käyttää lainsäädännöstä ja ohjeistuksista johtuen. Luvussa 4 on esitetty aineisto ja tutkimustulokset jotka osoittavat, että pilvipalveluiden käyttö olisi tietyissä tilanteissa mahdollista.

Pilvipalveluiden käyttöön liittyy lukuisia etuja ja haasteita. Pilvipalveluiden käytöllä on mahdollista saavuttaa sekä kustannussäästöjä että monia muita hyötyjä, joista osa liittyy poliisihallinnonalalle tärkeisiin tietoturvan ja käyttövarmuuden parantamiseen. Toisaalta pilvipalveluihin liittyy lukuisia haasteita ja riskejä joten vaikka pilvipalveluiden käyttämiseen siirtyminen on suositelta-

vaa, niin sen tulee tapahtua vähitellen ja riskianalyysejä tehden, jotta riskit pysyvät hallinnassa.

Tämän tutkimuksen perusteella voidaan sanoa, että poliisihallinnonalan operatiivisia tietojärjestelmiä, joissa käsitellään salassa pidettävää tietoa, voidaan viedä pilveen tietyt rajoitukset huomioiden. Nämä kohdistuvat ennen kaikkea siihen missä tietojärjestelmien kehitys ja ylläpito sekä tietojen käsittely että tallennus tapahtuvat. Jos pilvipalveluntarjoaja pystyy todistettavasti tarjoamaan nämä toiminnot Suomessa, niin pilvipalveluita voidaan käyttää.

Johtopäätöksenä poliisihallinnonalalle suositellaan pilvipalveluiden käytön aloittamista viemällä muutamia ST IV luokiteltuja tietojärjestelmiä pilvipalveluun, joka toteutetaan Suomessa. Jos julkisten pilvipalveluiden toimittajat eivät tarjoa selkeästi Suomeen rajautuvaa tuotantomallia, niin ainakin POHA:n tai Valtorin tuottama pilvipalvelu sopisi tarkoitukseen, jos sellaista olisi tarjolla. Esimerkiksi jos Valtori alkaa tarjota viranomaisille tarkoitettua yhteisöpilveä, niin tällaiseen olisi suositeltavaa lähteä mukaan ainakin joillain uusilla tietojärjestelmillä.

Salassa pidettävien tietojen yliluokittelu ST III ja ST IV välillä nousi myös esille yhtenä tutkimustuloksena. Johtopäätöksenä suositellaan kiinnittämään käytäntöihin ja ohjeistuksiin huomiota salassapidoista päätettäessä, koska tiedon ST-luokitus vaikuttaa paljon sen käsittelyyn ja tallentamiseen kohdistuviin tietoturvavaatimuksiin. Salassapitosäännökset ja niiden soveltaminen voisivat tarjota mielenkiintoisia jatkotutkimusmahdollisuuksia. Voisi olla hyödyllistä esimerkiksi testata jollain testiaineistoilla, että mille ST-luokituksille poliisihallinnonalan työntekijät niitä testitilanteissa sijoittaisivat ja millä perusteilla. Lisäksi tutkimuksen arvoista voisi olla haastatella luokituspäätöksiä tehneitä henkilöitä siitä, mitä kaikkia asioita he arvioivat tehdessään luokituspäätöksiä.

Toinen mielenkiintoinen jatkotutkimusaihe olisi vertailla Suomen tilannetta johonkin toiseen EU-maahan. Suomalainen lainsäädäntö on monin osin saanut vaikutteita Ruotsista, joten se voisi olla yksi mahdollinen vertailukohde. Toisaalta kansainvälinen poliisiyhteistyö on aktiivista Viron kanssa, joten vertailu virolaiseen säädösperustaan ja käytäntöihinsä voisi olla tutkimuksen arvoista. Eli jos jokin tieto täältä toimitetaan toiseen maahan jollekin ST tasolle luokiteltuna, niin miten samanlaista tai erilaista sen käsittely siellä on. Tai miten erilaisia säädöksiä ja ohjeistuksia sen käsittelyyn ja tallentamiseen siellä liittyy.

Tätä kirjoittaessa EU:n tietosuoja-asetuksen ja sen pohjalta tehtävän kansallisen säädöstyön vaikutukset poliisihallinnonalan toimintaan eivät ole vielä täysin selvillä. Lisäksi tietojen salassapitoon ja VAHTI-ohjeisiin on tulossa muutoksia. Mielenkiintoinen jatkotutkimusaihe olisi tehdä tämä tutkimus uudestaan muutamien vuosien kuluttua näiden muutoksien toteuttamisen ja jalkauttamisen jälkeen, että miten säädösperusta ja ohjeistukset ovat muuttuneet.

LÄHTEET

Aharony, N. (2015). An exploratory study on factors affecting the adoption of cloud computing by information professionals. The Electronic Library, 33(2), 308-323.

Aikat, J., Akella, A., Chase, J. S., Juels, A., Reiter, M. K., Ristenpart, T., Swift, M. (2017). Rethinking Security in the Era of Cloud Computing. IEEE Security Privacy, 15(3), 60–69.

Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2016, October). Security risk factors that influence cloud computing adoption in Saudi Arabia government agencies. In Information Society (i-Society), 2016 International Conference on (pp. 28-31). IEEE.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357-383.

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. MIS Quarterly.

Anita Saaranen-Kauppinen & Anna Puusniekka. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. <http://www.fsd.uta.fi/menetelmaopetus/>. (Viitattu 04.03.2018.)

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... & Zaharia, M. (2009). Above the clouds: A berkeley view of cloud computing (Vol. 17). Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley.

Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. Computers in Human Behavior, 45, 93-98.

Arora, S., & Banerji, G. (2016). Security Infrastructure of Cloud Computing. IITM Journal of Information Technology, 34.

Aubert, B. A., Patry, M., & Rivard, S. (1998, January). Assessing the risk of IT outsourcing. In System Sciences, 1998., Proceedings of the Thirty-First Hawaii International Conference on (Vol. 6, pp. 685-692). IEEE.

Chen, H., Wang, F. Y., & Zeng, D. (2004). Intelligence and security informatics for homeland security: information, communication, and transportation. IEEE Transactions on Intelligent Transportation Systems, 5(4), 329-341.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 39, 447-459.

Chou, D. C. (2015). Cloud computing risk and audit issues. Computer Standards & Interfaces, 42, 137-142.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. European Journal of Information Systems, 1-37.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, 20(1), 79-98.

Garcia, R., & Chow, C. E. (2015). Identity considerations for public sector hybrid cloud computing solutions. Teoksessa 2015 International Conference on Computer Communication and Informatics (ICCCI) (ss. 1–8).

Gashamia, J. P., Chang, Y., & Park, M. C. (2013). Cross-national study on factors affecting cloud computing adoption in the public sector: Focus on perceived risk. In Proceedings of Pacific Asia Conference on Information Systems.

Gashami, J. P., Chang, Y., Rho, J. J., & Park, M. C. (2014). Understanding the Trade-Off between Privacy Concerns and Perceived Benefits in SaaS Individual Adoption. In PACIS (p. 354).

Gil-Garcia, J. R., Chengalur-Smith, I., & Duchessi, P. (2007). Collaborative e-Government: impediments and benefits of information-sharing projects in the public sector. European Journal of Information Systems, 16(2), 121-133.

Ellram, L. M., Tate, W. L., & Billington, C. (2008). Offshore outsourcing of professional services: A transaction cost economics perspective. Journal of Operations Management, 26(2), 148-163.

Gottschalk, I., & Kirn, S. (2013). Cloud computing as a tool for enhancing ecological goals?. Business & Information Systems Engineering, 5(5), 299-313.

Haag, S., Eckhardt, A., & Kronung, J. (2014, January). From the Ground to the Cloud--A Structured Literature Analysis of the Cloud Service Landscape

around the Public and Private Sector. In System Sciences (HICSS), 2014 47th Hawaii International Conference on (pp. 2127-2136). IEEE.

Haimes, Y. Y., Crowther, K., & Horowitz, B. M. (2008). Homeland security preparedness: Balancing protection with resilience in emergent systems. Systems Engineering, 11(4), 287-308.

Jones, S. (2015). Cloud computing procurement and implementation: Lessons learnt from a United Kingdom case study. International journal of information management, 35(6), 712-716.

Jones, S., Irani, Z., Sivarajah, U., & Love, P. E. D. (2017). Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. Information Systems Frontiers, 1–24.

Kundra, V. (2011). Federal cloud computing strategy.

Li, S. H., Yen, D. C., Chen, S. C., Chen, P. S., Lu, W. H., & Cho, C. C. (2015). Effects of virtualization on information security. Computer standards & interfaces, 42, 1-8.

Metsämuuronen, J. (2011). Tutkimuksen tekemisen perusteet ihmistieteissä. Gummerus ja Booky. fi. Jyväskylän yliopisto, e-kirja, opiskelijalaitos.

Mohapatra, S. (2017). Cloud computing relationships between deployments model selection and it security (Doctoral dissertation, Capella University).

Mutkoski, S. (2015). National Cloud Computing Principles: Guidance for Public Sector Authorities Moving to the Cloud. Teoksessa 2015 IEEE International Conference on Cloud Engineering (s. 404–409).

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. Information and organization, 17(1), 2-26.

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. Government information quarterly, 27(3), 245-253.

Pelteret, M., & Ophoff, J. (2016). A Review of Information Privacy and Its Importance to Consumers and Organizations. Informing Science: the International Journal of an Emerging Transdiscipline, 19, 277-302.

Rajaeian, M. M., Cater-Steel, A., & Lane, M. (2016). IT outsourcing decision factors in research and practice: a case study. arXiv preprint arXiv:1606.01454.

Saaranen-Kauppinen, A. & Puusniekka, A. (2006 A). KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. <http://www.fsd.uta.fi/menetelmaopetus/kvali/L3_3_2.html>. (Viitattu 10.03.2018.)

Saaranen-Kauppinen, A. & Puusniekka, A. (2006 B). KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. <http://www.fsd.uta.fi/menetelmaopetus/kvali/L3_3_1.html>. (Viitattu 10.03.2018.)

Shin, D. H. (2013). User centric cloud service model in public sectors: Policy implications of cloud services. Government Information Quarterly, 30(2), 194-203.

Tripathi, S., & Nasina, J. (2017). Adoption of Cloud Computing in Business: A Multi-Case Approach to Evaluate the Fit-Viability Model (FVM). International Journal of Business and Information, 12(1), 39.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. Journal of Management Information Systems, 29(4), 263-290.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS quarterly, 37(1).

Vithayathil, J. (2017). Will cloud computing make the Information Technology (IT) department obsolete?. Information Systems Journal.

Whitley, E. A., Willcocks, L. P., & Venters, W. (2013). Privacy and Security in the Cloud: A Review of Guidance and Responses. Journal of International Technology & Information Management, 22(3).

Yang, H. L., & Lin, S. L. (2015). User continuance intention to use cloud storage service. Computers in Human Behavior, 52, 219-232.

Yang, H., & Tate, M. (2012). A descriptive literature review and classification of cloud computing research. CAIS, 31, 2.

Zhao, F., Gaw, S. D., Bender, N., & Levy, D. T. (2013). Exploring Cloud Computing Adoptions in Public Sectors: A Case Study. GSTF Journal on Computing (JoC), 3(1), 42.

LIITE 1 HAASTATTELURUNKO

Tämä liite sisältää tutkimuksessa käytetyn haastattelurungon viimeisimmän version.

Yleistä

Kun poliisissa päätetään, että hankitaan ja käyttöönotetaan uusi tietojärjestelmä, niin millainen prosessi se on? Mitä otetaan huomioon, kuka päättää?

Millaisia erilaisia pilvipalveluita on olemassa? Millaisia eroja niissä on?

Miten poliisihallinnossa suhtaudutaan pilvipalveluihin?

Onko poliisihallinnon tietojärjestelmiä tietääksesi toteutettu pilvipalveluissa? Jos on, niin millaisissa?

Poliisihallinnonalan erityisvaatimukset tietojärjestelmille

Miten koet poliisihallinnon vaatimuksien tietojärjestelmille eroavan yksityisen puolen vaatimuksista?

Mitkä ovat tärkeimmät lait ja asetukset jotka ohjaavat poliisihallinnon tietojärjestelmien kehittämistä ja ylläpitoa?

Mitkä ovat tärkeimmät ohjeistukset jotka ohjaavat poliisihallinnon tietojärjestelmien kehittämistä ja ylläpitoa?

Miten EU:n uusi tietosuojadirektiivi tulee vaikuttamaan poliisihallinnon tietojärjestelmiin?

Ovatko voimassaolevat ohjeet samat koko tietojärjestelmäprojektin ajan tai muuttuvatko ne kuinka usein tai yllättäen?

Millaisia lainsäädännöstä ja viranomaisten ohjeista tulevia erityisvaatimuksia järjestelmille on? Eroavatko nämä muita viranomaisia koskevista säädöksistä ja ohjeista?

Asettavatko lait, asetukset tai ohjeistukset poliisin tietojärjestelmille jotain sellaisia tietoturvaan tai yksityiseen liittyviä vaatimuksia, joita on vaikeaa tai mahdotonta toteuttaa? Jos kyllä, niin mitkä ja millaisia?

Miltä tahoilta poliisihallinnossa voi saada ohjeita tietojärjestelmien kehittämisessä huomioitavissa tietoturva-asioissa?

Mitä pitää huomioida tietojärjestelmien auditoimiseksi viranomaistarpeita vastaavaksi? Millaisia ongelmia auditointeihin liittyy?

Miten ST-luokittelu käytännössä toimii? Onko tietojen luokittelussa ja käsittelyssä ongelmia ja jos niin millaisia?

Olisiko tarpeen järjestää koulutusta tietojärjestelmien kehittämisestä poliisihallinnossa? Jos kyllä, niin keille ja millaista?

Pilvipalveluiden edut

Pitäisikö poliisihallinnon tietojärjestelmiä toteuttaa pilvipalveluissa nykyistä enemmän? Perustelut suuntaan tai toiseen?

Jos poliisihallinnon tietojärjestelmiä on toteutettu pilvipalveluissa, niin millaisia etuja sillä on haettu?

JOS ei ole toteutettu pilvipalveluissa tai ei osaa vastata niillä haettujen etujen osalta, niin kysytään, että:
Millaisia etuja poliisihallinnossa haetaan tietojärjestelmien kehittämisellä?

Onko näitä etuja saavutettu?

Miten on todennettu, että on saavutettu tai ei ole saavutettu?

Eli millaisia mittareita käytetään etujen mittaamiseen?

Jos vertaat pilvipalveluiden mahdollista käyttöä poliisin tietojärjestelmissä tai niiden käyttöä yleensä tietojärjestelmissä, niin voisivatko mielestäsi seuraavat pilvipalveluiden tarjoamat edut realisoitua poliisin tietojärjestelmissä? Halvempi ylläpito, laiteresurssien jakaminen, riskien siirtäminen, tietojen jaettavuus, saavutettavuus, järjestelmien yhteentoimivuus, pienten tietojärjestelmien toteuttaminen, varmuuskopiointi.

Pilvipalveluiden haasteet, Tietoturva ja -suoja ja yksityisyys yms.

Miten poliisissa suhtaudutaan tietoturvaan ja yksityisyydensuojaan?

Millaisia riskejä poliisin tietojärjestelmien tietoturvaan ja -suojaan kohdistuu?

Mitkä niistä ovat merkittävimpiä?

Millaisia pääsynhallintaan liittyviä riskejä poliisin tietojärjestelmiin kohdistuu?

Millaisia tiedon saatavuuteen liittyviä riskejä poliisin tietojärjestelmiin kohdistuu?

Millaisia tiedon eheyteen liittyviä riskejä poliisin tietojärjestelmiin kohdistuu?

Millaisia tietoturvatapahtumia poliisin tietojärjestelmiin on kohdistunut?

Millaiset ovat yleisimpiä tai eniten negatiivisia seurauksia aiheuttaneita tietoturvatapahtumia?

Miten poliisihallinnon työntekijöitä estetään lukemasta tietojärjestelmistä tietoja, jotka eivät liity heidän työtehtäviinsä?

Miten poliisihallinnossa huolehditaan siitä, että kullakin työntekijällä on oikeus vain niihin tietojärjestelmiin, joita hänen työnsä vuoksi tulee käyttää? Kuka huolehtii oikeuksien osittaisesta poistamisesta henkilöiden siirtyessä uusiin tehtäviin tai heidän työnkuvansa muuttuessa?

Miten estetään salassa pidettäviin tietoihin käsiksi pääseminen tietojärjestelmiä toimittavien yrityksien työntekijöiltä joilla on oikeudet johonkin tai joihinkin tietojärjestelmiin järjestelmien kehitystä tai ylläpitoa varten?

Olisiko tarpeen järjestää nykyistä enemmän koulutusta poliisihallinnon tietojärjestelmien kehitys- ja ylläpitotyössä työskenteleville tietoturvasta, yksityisyydensuojasta tms.? Jos kyllä, niin keille ja millaista?

Lopuksi kysymyksiä:

Millä edellytyksillä poliisin tietojärjestelmiä voidaan toteuttaa pilvipalveluissa?

Mitä muuta haluat sanoa haastattelussa käsiteltyihin aiheisiin liittyen?

Miten näet, tuleeko poliisi ottamaan enemmän pilvipalveluita käyttöön? Perustelut?

LIITE 2 KATAKRIN ST IV JA ST III VAATIMUKSIA

Liite 2 on suoraa lainausta Katakrista. Liitteeseen on koottu ne kohdat Katakrista, joissa esiintyy eroja ST IV ja ST III välillä vaatimuksissa.

Tietojen fyysiseksi suojaamiseksi tarvittavat alueet F 02

Suojaustason IV tietoja voidaan säilyttää hallinnollisella alueella. Suojaustason III-II tason tietoja tulee säilyttää turva-alueella.

Hallinnollinen alue

4) Alueella on selkeästi määritellyt näkyvät rajat, joilla henkilöt ja mahdollisuuksien mukaan ajoneuvot voidaan tarkastaa.
5) Alueelle on pääsy ilman saattajaa vain henkilöillä, joilla on lupa tulla alueelle. Kaikilla muilla henkilöillä on aina oltava saattaja tai heille on tehtävä vastaavat tarkastukset.
6) Mikäli alueella säilytetään salassa pidettäviä tietoja, alueella on kyseisen tiedon säilyttämiseen hyväksytty tila tai säilytysratkaisu.
7) Mikäli alueella käsitellään salassa pidettäviä tietoja, sivullisten pääsy tietoihin on estetty.

Turva-alue

8) Alueella on selkeästi määritellyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla.
9) Alueelle on pääsy ilman saattajaa vain henkilöillä, joilla on asianmukainen turvallisuusselvitys ja erityinen lupa tulla alueelle tiedonsaantitarpeensa perusteella. Kaikilla muilla henkilöillä on aina oltava saattaja tai heille on tehtävä vastaavat tarkastukset.
10) Aluetta rajaavat rakenteet muodostavat kokonaisuuden, joka tarjoaa riskeihin nähden riittävän suojan asiattoman pääsyn estämiseksi.
11) Mikäli alueella säilytetään salassa pidettäviä tietoja, tulee siellä olla kyseisen tiedon säilyttämiseen hyväksytty tila tai säilytysratkaisu.
12) Mikäli alueelle ei ole asennettu murtohälytysjärjestelmää ja alueella ei ole henkilöstöä palveluksessa ympäri vuorokauden, se on tarvittaessa tarkistettava normaalin työajan päätteeksi ja satunnaisin ajankohdin sen ulkopuolella.

Alueelle on laadittu turvallisuusmenettelyt, joissa on määräykset seuraavista:
15) Korkein suojaustaso- tai turvallisuusluokka, jota alueella voidaan käsitellä.
16) Sovellettavat valvonta- ja suojatoimenpiteet.
17) Henkilöt, joilla on pääsy alueelle ilman saattajaa tiedonsaantitarpeensa ja turvalli-

suusselvityksensä perusteella.
18) Henkilön saattamiseen liittyvät menettelyt.
19) Muut asiaan kuuluvat toimenpiteet ja menettelyt.

Hallinnollisen alueen raja:
Aluetta rajaavan aidan tai kuoren seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteilta ei vaadita erityisiä ominaisuuksia.
Hallinnollisen alueen raja ja salassa pidettävän tiedon käsittely- sekä säilytysyksikön rajaava tila tulisi olla lukittavissa lukolla, jonka avainten kopiointi on estetty patenttisuojalla.

Turva-alueen raja:

Suojaustaso III

Mikäli suojattavaa tietoa säilytetään tilassa hyväksytyssä säilytysyksikössä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden antaa sellainen rakenteellinen suoja, että niiden kautta alueelle tunkeutuminen on hidasta ja vaikeaa.

Mikäli suojattavaa tietoa säilytetään tilassa ilman hyväksyttyä säilytysyksikköä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden olla kyseisen suojaustason tiedon säilyttämiseen hyväksyttyä säilytysyksikköä vastaava. Tällainen säilytysyksikkö on SFS-EN-14450 luokan S2 turvakaappi tai vastaava. Tällaiseksi suojaksi voidaan katsoa myös esimerkiksi SFS-EN-1627 luokkaa 4 vastaava rakenteellinen suoja.

Tietoliikenneturvallisuus

Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen I 01

Hallinnollisen alueen raja:
Aluetta rajaavan aidan tai kuoren seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteilta ei vaadita erityisiä ominaisuuksia.
Hallinnollisen alueen raja ja salassa pidettävän tiedon käsittely- sekä säilytysyksikön rajaava tila tulisi olla lukittavissa lukolla, jonka avainten kopiointi on estetty patenttisuojalla.

Turva-alueen raja:

Suojaustaso III
Mikäli suojattavaa tietoa säilytetään tilassa hyväksytyssä säilytysyksikössä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden antaa sellainen rakenteellinen suoja, että niiden kautta alueelle tunkeutuminen on hidasta ja

vaikeaa.

Mikäli suojattavaa tietoa säilytetään tilassa ilman hyväksyttyä säilytysyksikköä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden olla kyseisen suojaustason tiedon säilyttämiseen hyväksyttyä säilytysyksikköä vastaava. Tällainen säilytysyksikkö on SFS-EN-14450 luokan S2 turvakaappi tai vastaava. Tällaiseksi suojaksi voidaan katsoa myös esimerkiksi SFS-EN-1627 luokkaa 4 vastaava rakenteellinen suoja.

Vähimpien oikeuksien periaate - Pääsyoikeuksien hallinnointi I 06

Toteutusesimerkki
Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t).
2) Järjestelmän käyttäjistä on olemassa lista.
3) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu.
4) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu.
5) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen.
6) Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen).
7) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti.
8) Tietojärjestelmissä salassa pidettävät tiedot on eritelty vähimpien oikeuksien periaatteen mukaisesti käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä.
9) Tietojärjestelmissä ko. suojaustason tiedot pidetään erillään julkisista ja muiden suojaustasojen tiedoista, tai eri tason tietoja käsitellään korkeimman suojaustason mukaisesti.
10) Tietojärjestelmissä tarkastusoikeuden varaavien tiedon omistajien tiedot säilytetään toisistaan ko. suojaustasolle viranomaisen hyväksymällä menetelmällä eroteltuna.

Suojaustasoilla III-II vaatimus voidaan täyttää siten, että kohtien 1-10 lisäksi toteutetaan seuraavat toimenpiteet:
11) Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Mikäli vaarallisia työyhdistelmiä syntyy, on niitä varten oltava valvontamekanismi.
12) Palvelimissa, työasemissa ja muissa tallennusvälineissä salassa pidettävät tiedot säilytetään viranomaisen ko. ympäristöön hyväksymällä menetelmällä salattuna (ks. I 12). Viranomainen voi hyväksyä tapauskohtaisesti myös korvaavan menettelyn, jossa salausvaatimus korvataan fyysisen ja loogisen pääsynhallinnan sekä tallennemedioiden hallinnan luotettavalla toteutuksella (ks. F 02, kohdat 6 ja 11). Huom: Korvaava menettely ei sovellu tilanteisiin, joissa salausta käytetään tarkastusoikeuden varaavien eri tiedon omistajien tietojen erotteluun.

Monitasoinen suojaaminen - Tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun alueen sisällä I 07

Toteutusesimerkki
Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet.
2) Kaikki käyttäjät tunnistetaan ja todennetaan.
3) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti.
4) Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen.
5) Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä/sovelluksissa ole teknisesti mahdollista, vaaditaan sovitut ja dokumentoidut salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille.
6) Todennus tehdään vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, a) käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, b) käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin.

Suojaustasoilla III-II vaatimus voidaan täyttää siten, että kohtien 1-5 lisäksi toteutetaan seuraavat toimenpiteet:
7) Edellytetään vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta.
8) Päätelaitteet tunnistetaan teknisesti (laitetunnistus, 802.1X, tai vastaava menettely) ennen pääsyn sallimista verkkoon tai palveluun, ellei verkkoon kytkeytymistä ole fyysisen turvallisuuden menetelmin rajattu suppeaksi (esim. palvelimen sijoittaminen lukittuun laitekaappiin teknisesti suojatun viranomaisen ko. suojaustasolle hyväksymän turva-alueen sisällä).

Suojaustason IV ympäristöissä, joissa uhka palvelunestohyökkäyksen aiheuttamiseen (tunnusten lukitseminen esim. Internet-kytkentäisissä tunnistuspalveluissa) arvioidaan merkittäväksi, tunnuksen lukittuminen voidaan korvata jollain riskiä pienentävällä menettelyllä (esim. vastaamisen hidastamiseen, suodattamiseen tai väliaikaiseen lukitsemiseen perustuvat menettelyt). Suojaustasolla IV ei yleensä edellytetä päätelaitteen teknistä tunnistamista, mikäli käyttäjät tunnistetaan.

Suojaustasojen III ja II menetelmät vahvasta käyttäjätunnistuksesta ja päätelaitteen tunnistamisesta voidaan joissain tapauksissa toteuttaa siten, että tietojärjestelmään on mahdollista päästä vain tiukasti rajatusta fyysisesti suojatulta alueelta (yleensä teknisesti suojattu turva-alue, lukittu laitekaappi, tai vastaava), jonka pääsynvalvonnassa käytetään vahvaa, vähintään kahteen tekijään perustuvaa tunnistamista. Tällöin käyttäjän tunnistaminen tietojärjestelmässä voidaan järjestää käyttäjätunnus-salasana -parilla.

Vähimmäistoimintojen ja vähimpien oikeuksien periaate - Järjestelmäkovennus I 08

Toteutusesimerkki
Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
Verkon aktiivilaitteet
1) Oletussalasanat on vaihdettu organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin.
2) Vain tarpeellisia verkkopalveluita on päällä ja nämä palvelut on rajattu vain tarpeellisiin verkkoliittymiin.
3) Verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset.
4) Hallinta ei ole mahdollista ilman käyttäjän tunnistamista ja todentamista.
5) Hallintayhteyksissä tulisi käyttää istuntojen aikakatkaisua.
6) Kovennukset pohjautuvat johonkin luotettavaksi arvioituun kovennusohjeeseen tai suositukseen.
Palvelimet, työasemat ja vastaavat
7) Tarjottavat (erityisesti verkko)palvelut on minimoitu ja rajattu vain välttämättömiin. On lisäksi käytössä verkkoliikenteen vain välttämättömään rajaava (host-based) palomuuriratkaisu.
8) Alusta sisältää vain järjestelmän tarvitsemia ohjelmistokomponentteja. Alustan komponenttien, prosessien (esim. palvelinprosessit), hakemistojen ja lisäohjelmien käyttöoikeudet on asetettu tarkoituksenmukaisiksi vähimpien oikeuksien periaatteen mukaisesti.
9) Käyttöjärjestelmään ja sovellusohjelmistoihin on asennettu tarpeelliset turvapäivitykset.
10) Järjestelmiin asennuksen yhteydessä automaattisesti luoduille tileille (esim. ”administrator” ja ”guest”) on oikeudet rajattu minimiin tai poistettu käytöstä.
11) Oletussalasanat on vaihdettu organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin.
12) Järjestelmä lukittuu automaattisesti, jos sitä ei käytetä vähään aikaan (esim. salasanasuojattu näytönsäästäjä aktivoituu 15 minuutin käyttämättömyyden jälkeen).
13) Käyttöoikeudet asetettu vähimpien oikeuksien periaatteen mukaisesti (vrt. I 06).
14) Käyttöjärjestelmän tunnettuja turvallisuusuhkia sisältävät automaattisen ohjelmakoodin suorituksen mahdollistavat ominaisuudet on kytketty pois päältä (erityisesti PDF-tiedostojen automaattinen esikatselu sekä ”autorun” ja ”autoplay”-toiminnallisuudet, sekä esimerkiksi USB- ja Firewire-laitteiden automaattisen käynnistymisen estäminen koneen ollessa lukittuna).
15) Ohjelmistot, erityisesti web-selaimet, PDF-lukijat, toimisto-ohjelmistot ja sähköpostiohjelmistot, ovat turvallisesti konfiguroituja. Ohjelmistojen kovennuksissa tulisi huomioida erityisesti ajettavan koodin (esim. JavaScript sekä makrot) oletusarvoisen suorittamisen estäminen.
16) BIOS-asetuksiin pääsy on suojattu salasanalla (suojaustasolla IV erityisesti Naton turvallisuusluokitellun tiedon osalta).
17) Järjestelmän tukemia lisäturvallisuusominaisuuksia (esimerkiksi DEP / ASLR / Applocker / SELINUX) hyödynnetään.

Suojaustasoilla III-II vaatimus voidaan toteuttaa siten, että kohtien 1-17 lisäksi toteutetaan seuraavat toimenpiteet:
Verkon aktiivilaitteet
18) Tarpeettomat verkkopistokkeet ja muut vastaavat tietoliikenneyhteydet on poistettu käytöstä.
Palvelimet, työasemat ja vastaavat
19) käyttöjärjestelmät ja muut ohjelmistot konfiguroidaan siten, että päivitykset haetaan vain tähän tarkoitukseen tarkoitetuista lähteistä ja kaikki tarpeeton verkkoliikennöinti on poistettu käytöstä (tavoitteena tehokkaamman poikkeamien havainnointikyvyn mahdollistaminen).
20) BIOS-asetukset on asetettu turvallisuutta tehostaviksi ja asetusten muuttaminen on estetty valtuuttamattomilta käyttäjiltä. Salasanasuojauksen lisäksi:
a) On sallittu vain ensisijaiselta kovalevyltä käynnistys. b) Tarpeettomat palvelut ja portit on poistettu käytöstä

Monitasoinen suojaaminen - Haittaohjelmasuojaus I 09

Toteutusesimerkki
Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat alttiita haittaohjelmatartunnoille.
2) Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä.
3) Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja ja hälytyksiä.
4) Haittaohjelmatunnisteet (ja vast.) päivittyvät säännöllisesti.
5) Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta.
6) Haittaohjelmahavaintoja sekä hälytyksiä seurataan säännöllisesti ja niihin reagoidaan.
7) Organisaatiossa suodatetaan haittaliikennettä vähintään sähköpostin ja WWW-liikenteen yhdyskäytävissä.

Suojaustasoilla III-II vaatimus voidaan täyttää siten, että kohtien 1-7 lisäksi toteutetaan seuraavat toimenpiteet:
8) Arvioidaan tarve järjestelmien USB-porttien ja vastaavien liityntöjen käytölle.
9) Tilanteissa, joissa liityntöjen käytölle ei ole kriittistä tarkastelua kestävää perustetta, liitynnät poistetaan käytöstä.
10) Tilanteissa, joissa liityntöjen käytölle on kriittistä tarkastelua kestävät perusteet, arvioidaan tapauskohtaisesti edellytykset ja ehdot, minkä mukaisia laitteistoja ja välineitä (esim. USB-muisteja) järjestelmään voidaan kytkeä.

Monitasoinen suojaaminen - Turvallisuuteen liittyvien tapahtumien jäljitettävyys I 10

Toteutusesimerkki
Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Tallenteet ovat riittävän kattavia tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen.
2) Keskeiset tallenteet säilytetään vähintään 6 kk, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa.
3) Lokitiedot ja niiden kirjauspalvelut suojataan luvattomalta pääsyltä (käyttöoikeushallinto, looginen pääsynhallinta).
4) Toimintaan on jalkautettu kirjallinen lokien keräys-, luovutus-, hälytys- ja seurantapolitiikka/-ohje, joka on muodostettu ottaen huomioon toiminnan vaatimukset.

Suojaustasoilla III-II vaatimus voidaan täyttää siten, että kohtien 1-4 lisäksi toteutetaan seuraavat toimenpiteet:
5) Keskeiset tallenteet säilytetään vähintään 2-5 vuotta, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa.
6) Lokitiedot varmuuskopioidaan säännöllisesti.
7) Samalla turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot on synkronoitu sovitun ajanlähteen kanssa.
8) On olemassa menetelmä lokien eheyden (muuttumattomuuden) varmistamiseen.
9) Syntyneiden lokitietojen käytöstä ja käsittelystä muodostuu merkinnät.

Monitasoinen suojaaminen - Hajasäteily (TEMPEST) I 14

Suojaustasolla IV ei ole erityisiä vaatimuksia. Suojaustasolla III-II raja-arvot ylittävän hajasäteilyn osalta suojautuminen toteutetaan ko. suojaustasolle viranomaisen hyväksymillä menettelyillä.

Salassa pidettävien tietojen välitys fyysisesti suojattujen alueiden välillä - Aineiston välitys postilla ja kuriirilla I 16

Toteutusesimerkki
Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Aineisto pakataan suljettavaan kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää suojaustasosta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän salassa pidettävää aineistoa (kirjekuoren tai vastaavan on oltava läpinäkymätön).
2) Aineisto toimitetaan kotimaassa tavallisena postina, kirjattuna kirjeenä tai viranomaisen ko. suojaustasolle hyväksymän kuriirimenettelyn mukaisesti. Ulkomaille toimitus postin välityksellä vain viranomaisen erillishyväksyntään pohjautuen.

3) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä henkilöstöä.
4) Organisaatiossa on tunnistettu vaatimukset ja toteutettu menettelyt erityissuojattavien tietoaineistojen (esimerkiksi salausavaimet) välittämiseksi.

Suojaustasolla III vaatimus voidaan täyttää siten, että kohdan 4 lisäksi toteutetaan seuraavat toimenpiteet:
5) Aineisto pakataan suljettavaan kaksinkertaiseen kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää suojaustasosta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän salassa pidettävää aineistoa (kirjekuorien tai vastaavien on oltava läpinäkymättömiä).
6) Aineisto toimitetaan kotimaassa viranomaisen erillishyväksyntään pohjautuen kirjattuna kirjeenä tai viranomaisen ko. suojaustasolle hyväksymän kuriirimenettelyn mukaisesti. Ulkomaille toimitus postin välityksellä voi tapahtua vain viranomaisen erillishyväksyntään pohjautuen.
7) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä turvallisuusselvitettyä henkilöstöä.

Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Turvallisuustarkoituksia varten tapahtuva salassa pidettävien tietojen kirjaaminen I 18

Suojaustaso IV
1) Tietojenkäsittely-ympäristössä toteutetaan hallinnolliset ja tekniset toimenpiteet, jotka koskevat salassa pidettävien tietojen valvomista koko niiden elinkaaren ajan, jotta autetaan estämään ja havaitsemaan tällaisten tietojen tahallinen tai tahaton vaarantuminen tai katoaminen.

Suojaustaso III-II
Kohdan 1 lisäksi
2) Salassa pidettävää tietoa käsitteleville organisaatioyksiköille on määritelty kirjaamo/rekisteröintipiste. Kirjaamot/rekisteröintipisteet on perustettu fyysisille ko. suojaustason vaatimukset täyttäville turva-alueille.
3) Salassa pidettävä tieto kirjataan/rekisteröidään sille tarkoitetuissa kirjaamoissa/rekisteröintipisteissä, kun aineisto saapuu organisaatioyksikköön tai lähtee siitä.
4) Asiakirjojen käsittely kirjataan sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai asiakirjaan.

Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Salassa pidettävää tietoa sisältävien tietoaineistojen hävittäminen I 19

Suojaustaso IV
1) Ei-sähköisten aineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.
2) Sähköisten aineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käyte-

tään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.
3) Tietojärjestelmien käytön yhteydessä syntyvät tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti, jolleivät ne poistu tietojärjestelmästä automaattisesti.

Suojaustaso III
Kohtien 1-3 lisäksi
4) Sekä kirjaajan että todistajan, jos jälkimmäisen läsnäoloa vaaditaan, on allekirjoitettava hävittämistodistus, joka tallennetaan kirjaamoon / rekisteröintipisteeseen. Kirjaamon / rekisteröintipisteen on säilytettävä aineistojen hävittämistodistukset vähintään viiden vuoden ajan.

Salassa pidettävien tietojen käsittely fyysisesti suojattujen alueiden sisällä - Fyysinen turvallisuus I 21

Suojaustaso IV
1) Fyysiset turvatoimet toteutetaan kaikissa tiloissa, rakennuksissa, toimistoissa, huoneissa ja muissa paikoissa, joissa tietoja käsitellään tai säilytetään, tietojenkäsittelyympäristöjen sijoitusalueet mukaan luettuina.
2) Tietojen käsittely on mahdollista turva-alueilla, hallinnollisella alueella tai viranomaisen hyväksymillä menettelyillä hallinnollisen alueen ulkopuolella.
3) Tietojen säilytys on mahdollista turva-alueilla ja hallinnollisella alueella soveltuvissa lukittavissa toimistokalusteissa, tai tilapäisesti myös viranomaisen hyväksymillä menettelyillä hallinnollisen alueen ulkopuolella.

Suojaustaso III-II
1 kohdan lisäksi:
4) Tietojen käsittely on mahdollista viranomaisen hyväksymillä turva-alueilla. Tietojen käsittely on mahdollista myös hallinnollisilla alueilla, jos pääsy salassa pidettäviin tietoihin on suojattu sivullisilta.
5) Tietojen säilytys on mahdollista viranomaisen hyväksymillä turva-alueilla turvasäilytysyksikössä tai kassaholvissa.

Salassa pidettävien tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä - Etäkäyttö ja etähallinta I 22

Suojaustaso IV
1) Tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä on mahdollista vain viranomaisen ko. suojaustasolle hyväksymien korvaavien menettelyjen mukaisesti.
2) Henkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön / -hallintaan.
3) Elleivät hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolelle viedyt suojaustason IV tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattu viranomaisen ko. suojaustasolle hyväksymällä menetelmällä, tietovälineet säilytetään vastaavantasoisesti suojaten, kuin hallinnollisen turva-alueen lukittavissa toimistokalusteissa

säilytettynä, tai tietovälineitä ei jätetä valvomatta.
4) Järjestelmien etäkäyttö-/-hallintaratkaisu edellyttää viranomaisen ko. suojaustasolle hyväksymää liikenteen salausta.

Suojaustaso III-II
Kohtien 1-2 ja 4 lisäksi:
5) Hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolelle viedyt salassa pidettävää tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ovat koko ajan kuljettajansa hallussa, ellei niitä ole salattu viranomaisen ko. suojaustasolle hyväksymällä menetelmällä. Salassa pidettäviä tietoja ei avata matkalla eikä lueta julkisilla paikoilla.
6) Järjestelmien etäkäyttö/-hallinta rajataan viranomaisen hyväksymälle fyysisesti suojatulle alueelle.

Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Ohjelmistohaavoittuvuuksien hallinta I 23

Toteutusesimerkki
Suojaustasoilla IV vaatimus voidaan toteuttaa siten, että toteutetaan alla mainitut toimenpiteet:
1) Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti.
2) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat tarkastetaan vähintään (haavoittuvuusskannaus, CMDB, jne.) vuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. Lisäksi säännöllisesti (esim. kuukausittain) tarkastellaan keskitetyistä päivityksenjakopalveluista päivitysten asentumisen onnistumista.
Suojaustasoilla III ja II vaatimus voidaan toteuttaa siten, että kohdan 1 lisäksi toteutetaan seuraava toimenpide:
3) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat tarkastetaan vähintään (haavoittuvuusskannaus, CMDB, jne.) puolivuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. Lisäksi säännöllisesti (esim. kuukausittain) tarkastellaan keskitetyistä päivityksenjakopalveluista päivitysten asentumisen onnistumista.

Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - varmuuskopiointi I 24

Toteutusesimerkki
Suojaustasoilla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Varmuuskopiot käsitellään ja säilytetään niiden elinkaaren ajan vähintään ko. suojaustason järjestelmissä.
2) Käsiteltäessä samalla varmistusjärjestelmällä tarkastusoikeuden varaavien eri omistaji-

en tietoja, tarkastusoikeuden (vrt. I 06) mahdollistavat erottelumenettelyt on toteutettava ko. suojaustason mukaisesti varmistusjärjestelmän liittymien ja tallennemedioiden osalta.
3) Mikäli varmuuskopioita siirretään ko. suojaustason fyysisesti suojatun alueen ulkopuolelle, menettelyt kuin I 15:ssa (sähköinen välitys) ja/tai I 16 sekä I 22 (kuljetus fyysisesti suojatun alueen ulkopuolelle).
4) Varmistusmediat hävitetään ko. suojaustason mukaisesti (I 19). Suojaustasolla III-II vaatimus voidaan toteuttaa siten, että kohtien 1-4 lisäksi toteutetaan seuraava toimenpide:
5) Varmuuskopioista on rekisterit ja varmuuskopioiden käsittely tulisi kirjata sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai asiakirjaan.