Teemu Reponen

PILVIPALVELUIDEN LAKITEKNISET RAJOITTEET JA KÄYTÄNTEET – JULKINEN SEKTORI

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Reponen, Teemu
Pilvipalveluiden lakitekniset rajoitteet ja käytänteet – Julkinen sektori
Jyväskylä: Jyväskylän yliopisto, 2021, 46 s.
Tietojärjestelmätiede, Pro Gradu
Ohjaaja: Siponen, Mikko

Pilvipohjaiset palvelut ovat nousseet useiden yrityksien toimintaan mukaan niiden kustannustehokkuuden sekä helpon tiedonsiirtelyn takia. Julkisissa organisaatioissa siirtymä on kuitenkin ollut huomattavasti hitaampaa ja useissa paikoissa vielä kesken. Julkiset organisaatiot käsittelevät myös paljon ei-julkista tietoa, mille tietoturvavaatimukset ovat huomattavan korkeat. Erityisesti GDPR, Schrems II sekä muut lait ja päätökset asettavat tiukat raamit tiedonkäsittelylle. Tämä tutkielma keskittyy julkisten organisaatioiden kohtaamiin vaatimuksiin sekä lakien asettamiin rajoitteisiin pilvipalveluiden käytössä. Tutkielma esittelee myös uhkia sekä teknisiä ratkaisuja joita pilvipalveluissa kohdataan. Tämän lisäksi tutkielman empiirinen osio luo katsauksen alalla vallitseviin käytänteisiin kyselytutkimuksen avulla. Tutkimuksen tuloksena on näkemys tämänhetkisiin käytänteisiin. Tämän lisäksi tutkielma antaa pohjan tulevaisuuden tutkimukselle erityisesti sopimuksiin liittyviin käytänteisiin.

Asiasanat: pilvipalvelu, tietoturva, luotettavuus, tietoturvauhkat, GDPR

ABSTRACT

Reponen, Teemu
Cloud service legal restrictions and practices – Public sector
Jyväskylä: University of Jyväskylä, 2021, 46 s.
Information systems science, Masters' thesis
Supervisor: Siponen, Mikko

Cloud based services have risen as an effective solution to manage their data for many commercial companies, because they are cost-effective and easy to use. However, for public organisations this transition has been much slower and is still in progress in some places. The problem for public organisations is that they manage a lot of non-public information, which has a high standard of security. Especially the adoption of GDPR, the recent Schrems II decision and other laws that regulate information security put a short leash on public organisations. This thesis focuses on public organisations and the challenges they face with navigating the sea of regulations that should be followed. Furthermore, this thesis presents the threats and some solutions that are often faced with using a cloud service. The empirical portion of this study focuses on the practices that public organisations have currently regarding the acquisition, contracts and use of cloud services. The result of this study is an overview on the current practices in the public sector. In addition, the study sets a strong basis for further research on the subject and especially the contractual side of using a cloud service.

Keywords: cloud service, information security, information security threats, accountability, GDPR

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tiedonhallinta on nykypäivänä yksi suurimmista ongelmista tietotekniikassa. Tietoa luodaan jatkuvasti kiihtyvällä tahdilla ja sen käsittelyyn sekä tallentamiseen on kehitetty useita palveluita, joista suurin osa tällä hetkellä perustuu pilvipalveluihin. Viestintävirasto (2014) määrittelee **pilvipalvelut** vastaavasti: ” […] verkkoyhteyden välityksellä tarjottavia tietojenkäsittely- ja -tallennuspalveluita sekä tietoliikennepalveluita.” Useimmat yksityiset henkilöt käyttävät pilvipalveluita jossain muodossa jokapäiväisessä elämässään, mutta yrityksille pilveen siirtyminen ei ole yhtä helppoa.

Pilvipalveluiden vetovoima perustuu kustannustehokkuuteen sekä helppokäyttöisyyteen. Yrityksille pilvipalvelu on kuitenkin paljon enemmän kuin tallennustila, joten vaatimusten taso on korkeampi kuin normaalilla käyttäjällä. Tämän lisäksi yritysten riski tietomurtojen sattuessa on huomattavasti suurempi ja saattaa aiheuttaa suurta taloudellista vahinkoa. Tietoturva on siis yrityksille ensisijaisen tärkeää ja saattaa rajoittaa yritysten halua siirtyä pilvipalveluihin. Amerikkalainen National Institute of Standards and Technology, määrittelee **tietoturvallisuuden** vastaavasti: ”Tiedon sekä tietojärjestelmien suojaamista luvattomalta pääsyltä, käytöltä, julkistamiselta, häiriöiltä, muokkaamiselta tai tuhoamiselta, jotta voidaan taata luottamuksellisuus, eheys sekä saatavuus” (Kissel, 2011, s. 94). Kuten tästä määritelmästä selviää, tietoturvallisuus käsittää erittäin laaja-alaisesti uhkia jotka eivät rajoitu vain ulkopuolisiin hyökkäyksiin. Pilvipalveluiden tietoturvan sekä tiedonkäsittelyn luotettavuuden määrittäminen on erityisesti yritysten näkökulmasta tärkeää.

Julkisella sektorilla, kuten kunnissa sekä kaupungeissa, on myös herätty pilvipalveluiden hyötyihin ja niiden käyttö yleistyy jatkuvasti. Kunnat ja kaupungit kuitenkin kohtaavat samat ongelmat kuin yritykset, eli haasteet tietoturvan kannalta ja julkisen sektorin toimijoihin kohdistuu vielä tarkempi valvonta. Tiedonkäsittelyä valvotaan paitsi valtion toimesta, niin myös EU:n tasolta EU:n tietosuoja-asetus **GDPR**:n avulla. Suomen tietosuojavaltuutetun toimisto määrittelee GDPR:n vastaavasti: EU:n luoma yleinen tietosuoja-asetus,

joka on ”[..] henkilötietojen käsittelyä säätelevä laki.” (Tietosuojavaltuutetun toimisto, (2020))

Tämä tutkimus vastaa kirjallisuuskatsauksen avulla seuraavaan tutkimuskysymykseen:

- Mitä rajoitteita lait ja valtion linjaukset asettavat pilvipalveluiden käytölle?

Kirjallisuuskatsauksen jälkeen toteutetaan empiirinen osio, joka koostuu kyselytutkimuksesta tietoturvan sekä tiedonhallinnan ammattilaisille. Empiirinen osio vastaa tutkimuksen toiseen tutkimuskysymykseen:

- Millaisia käytänteitä julkisella sektorilla on pilvipalveluiden hankinnassa sekä käytössä?

Kirjallisuuskatsauksen tavoitteena on löytää lähdekirjallisuudesta konkreettisia esimerkkejä siitä miten lainsäädännöllä sekä suosituksilla voidaan kontrolloida tiedonkäsittelyä pilvipalveluissa. Toisaalta kirjallisuuskatsaus myös kuvaa pilvipalveluiden teknistä toteutusta antaakseen lukijalle näkemyksen pilvipalveluiden toiminnasta. Lähdekirjallisuudesta löytyvät valtavat määrät tietoturvauhkia sekä pilvipalveluiden alati jatkuva kehitys luovat tarpeen tälle tutkimukselle. Aihetta on tutkittu paljon, mutta pilvipalveluiden toiminta ja käyttötarkoitus muuttuvat jatkuvasti, joten uusia uhkia sekä ratkaisuja tulee tutkia jatkuvasti.

Kirjallisuuskatsaus toteutettiin käyttämällä eri tietokantoja tieteellisten lähteiden hakuun. Pääasiallisesti tutkimuksessa käytettiin Jyväskylän yliopiston JYKDOK-palvelua, mutta lähteitä haettiin myös Scopuksesta, IEEE:n tietokannoista sekä Elsevierista. Google Scholaria käytettiin lähteiden viittausmäärien tarkistamiseen, jos se ei selvinnyt itse tietokannasta. Lähteiden hakua rajattiin lähteisiin, jotka olivat vertaisarvioituja sekä saatavilla kokonaan. Pääasiallisia hakusanoja tiedonhaussa olivat: ”Cloud computing”, ”GDPR”, ”Legislation” ja ”Security threats”. Lähteitä arvioitiin niiden julkaisuvuoden, julkaisijan, viittausmäärien sekä tiivistelmän perusteella. Yli 10 vuotta vanhat lähteet hylättiin, elleivät ne tarjonneet teoreettista taustaa, joka ei ollut vanhentunut. Julkaisijoiden arvioinnissa käytettiin apuna Julkaisufoorumin arvioita julkaisijan luotettavuudesta. Lähteissä esitettyjen asioiden oikeellisuuden arvioinnissa käytettiin apuna ilmoitettuja määriä siitä, kuinka monta kertaa lähteeseen on viitattu. Lähteet, joihin ei ollut viitattu kertaakaan aikaisemmin hylättiin, sillä koettiin etteivät ne ole tarpeeksi luotettavia. Melkein kaikki lähteet ovat vertaisarvioituja tieteellisiä lähteitä, mutta joitakin määritelmiä sekä lakiteknisiä asioita on myös haettu esimerkiksi Euroopan unionin kotisivuilta.

Tutkimus on jaettu kuuteen sisältölukuun, joista ensimmäinen on Pilvipalvelut. Ensimmäinen sisältöluku luo teoreettista taustaa pilvipalveluiden toiminnasta ja toimijoista. Ilman toiminnan ja toimijoiden taustoittamista on vaikea ymmärtää mahdollisia uhkia sekä niihin luotuja ratkaisuja.

Ensimmäinen sisältöluku on lyhyt, sillä sen on tarkoitus luoda nopea katsaus pilvipalveluihin.

Toisessa sisältöluvussa on esitelty lähdekirjallisuudessa yleisimmin esiintyneet uhkat pilvipalveluille. Toisaalta myös käyttäjien vastuuta tutkitaan, eli sitä kuinka asiakasyrityksen johto sekä työntekijät pystyvät osaltaan vaikuttamaan pilvipalveluiden tietoturvallisuuteen. Uhkien ymmärtäminen antaa valmiudet ymmärtää niitä varten luodut ratkaisut sekä hyvien käytänteiden merkitys.

Neljännessä sisältöluvussa käydään läpi yritysten välisiä sopimuksia, lainsäädäntöä sekä säännöksiä, jotka vaikuttavat pilvipalveluiden toimintaan. Erityisesti neljäs sisältöluku keskittyy EU:n tietosuojadirektiivin GDPR:n sekä Suomen valtion pilvipalvelulinjauksiin. Tämä luku valmistaa lukijan empiiristä tutkimusta varten.

Viidennessä sisältöluvussa esitellään tutkimusmenetelmä ja tutkimuksen tavoitteet. Tämän lisäksi luvussa käydään läpi vielä hieman teoreettista taustaa tutkimukselle. Lopuksi luvussa keskustellaan datan keräämisen prosessista.

Kuudes luku esittelee empiirisen tutkimuksen tulokset ja ne analysoidaan. Tulokset on jaoteltu käyttöön liittyviin käytänteisiin sekä sopimusten ja hankinnan käytänteisiin. Tämän luvun lopussa keskustellaan tuloksista yleisellä tasolla ja mietitään tutkimuksen onnistumista sekä kohdattuja haasteita.

Seitsemäs luku on yhteenveto koko tutkimuksesta. Luvussa kerrataan vielä tutkimuskysymykset sekä keskustellaan tutkimuksen onnistumisesta ja tuloksista. Lopuksi käydään läpi tulevaisuuden tutkimusaiheita ja esitellään tutkimuksen haasteet.

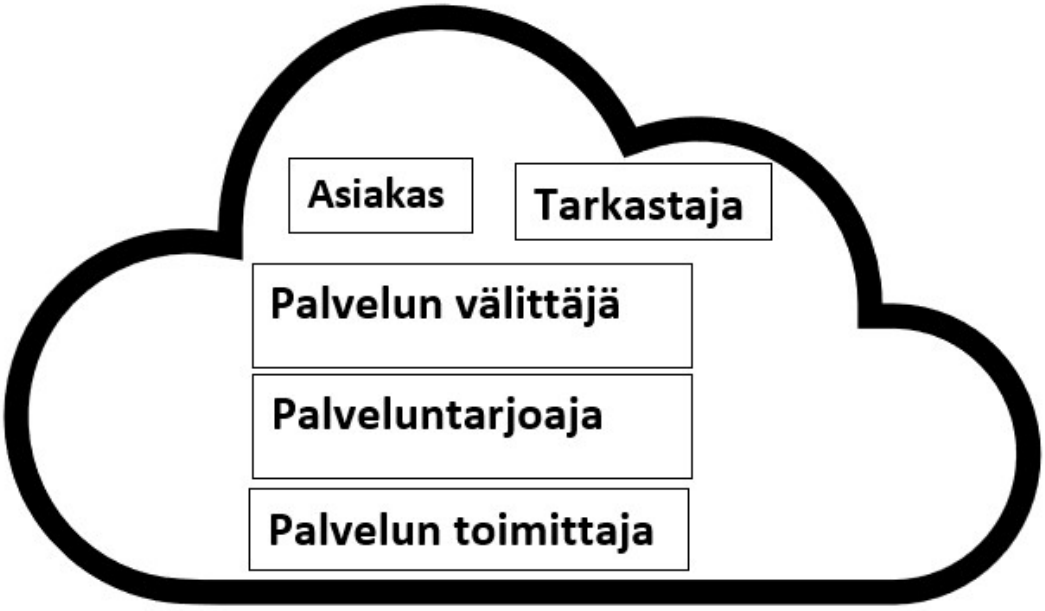
2 PILVIPALVELUT

Tässä luvussa esitellään pilvipalveluiden toimintaa, sekä sitä miksi näiden palveluiden käyttö on yrityksille kannattavaa. Lisäksi kuvataan pilvipalveluiden tietoturvan teknistä toteutusta.

2.1 Pilvipalvelun toiminta

Pilvipalveluita käytetään lähes kaikkialla jokapäiväisessä elämässä, sillä suuri osa palveluista, kuten sähköpostit, pohjautuvat pilvipalveluihin. Myös useimmat puhelinvalmistajat tarjoavat pilvitallennustilaa asiakkaillensa, esimerkiksi Applen iCloud sekä Android puhelimissa Google Drive. Pilvipalveluiden toiminnan ymmärtäminen on tärkeää, jotta voidaan ymmärtää niiden tarjoamat mahdollisuudet sekä ongelmat.

Pilvipalvelun muotoja on useita, mutta toimijat niissä pysyvät samoina. Ravi Kumar, Herbert Raj sekä Jelciana (2018) esittelevät 5-osaisen mallin kuvaamaan pilvipalveluiden eri toimijoita (ks. kuvio 1).



KUVIO 2 Pilvipalvelumalli (Uudelleen piirretty Ravi Kumar ym., 2018, s. 692)

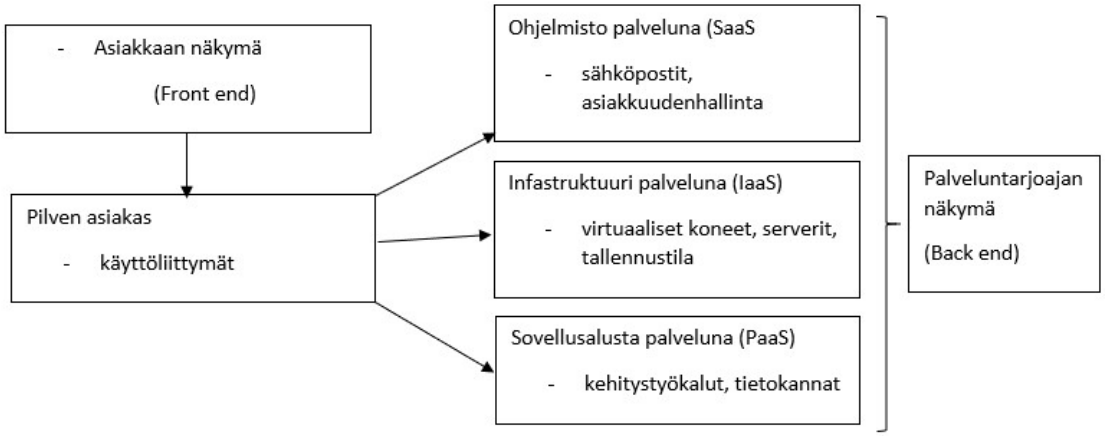
Pilvipalveluiden toimintamallissa asiakas maksaa palvelusta, jonka palveluntarjoaja toimittaa. Palveluntarjoajan ja asiakkaan välissä toimii palvelun välittäjä, joka välittää eli myy tuotteen asiakkaalle. Palveluntarjoajan alaisuudessa toimii palvelun toimittaja, joka vastaa pilven toiminnallisuudesta. Viimeiseksi, palvelun tarkastaa ulkopuolinen yksityinen tekijä, jotta palvelun luotettavuus voidaan määritellä puolueettomasti (Ravi Kumar ym., 2018). Ulkopuolinen tarkastus on osa pilvipalveluiden tietoturvaa sekä luotettavuutta edistäviä keinoja ja sen tarkoitus on auttaa asiakkaita valitsemaan luotettavia palveluita. Prosessi on teoriassa monimutkainen, mutta käytännössä pilvipalveluiden käyttäjiin vetoaa pilvipalveluiden helppokäyttöisyys.

2.2 Pilvipalveluiden käyttö

Pilvipalveluista on neljä yleisesti hyväksyttyä käyttöönottomallia: julkinen, yksityinen, hybridi sekä yhteisöllinen. (Kezia Rani, Padmaja Rani & Babu, 2015) Yksityinen pilvipalvelu on teoriassa turvallisempi kuin julkinen, mutta julkinen pilvipalvelu on kustannustehokkaampi. Yksityisellä pilvipalvelulla viitataan yrityksen sisäisiin datakeskuksiin, jotka eivät ole julkisesti saatavilla. (Armbrust ym., 2010) Tämä tutkimus tulee keskittymään yksityisten pilvipalveluiden toimintaan, sillä palvelut, jotka tarvitsevat tietoturvaa ovat usein toteutettu yksityisellä mallilla. Hybridi yhdistää nämä, eli yrityksen käytössä on kaikille asiakkaille suunnattu julkinen pilvi, mutta myös yksityinen pilvi. Pilvipalveluiden käytössä on tavoitteena, paitsi kilpailuedun saaminen, niin myös kustannustehokkuus. (Garrison, Kim & Wakefield, 2012) Tästä johtuen

yrityksille on ensisijaisen tärkeää onnistua luotettavan ja turvallisen pilvipalvelun valinnassa, mutta myös sen käyttöönotossa.

Pilvipalvelut jakautuvat kolmeen eri palvelumalliin: IaaS, PaaS sekä Saas (ks. kuvio 2). Yritykset hyötyvät näistä palveluista, koska niiden käyttö on helppoa ja tiedot ovat usein vain yhden käyttöliittymän takana.



KUVIO 3 Pilvipalveluiden rakenne (Uudelleen piirretty Rani ym., 2015, s.25)

Palvelumalleista useimmiten käytetään joko SaaS, eli sovellus palveluna, tai IaaS, eli infrastruktuuri palveluna -mallia. Sovellus palveluna sopii pienemmille yrityksille, jotka tarvitsevat apua taloushallinnon kanssa tai muun päivittäisen toiminnan kanssa, eikä kyseinen palvelu vaadi käyttäjältä juurikaan tietoteknistä osaamista. Toisaalta infrastruktuuri palveluna sopii suuremmille yrityksille ja vastuu datan hallinnasta on itse yrityksellä. Viimeisenä PaaS, eli sovellusalusta palveluna, jota voidaan käyttää pohjana sovelluskehitykselle sekä apuna vähentämään ylläpitokustannuksia. (Kezia Rani ym., 2015) Kaikissa palvelumalleissa on haasteita tietoturvallisuuden kanssa ja palveluntarjoajan valinta on ensisijaisen tärkeää.

Pilvipalveluissa hyödynnetään virtuaalisia koneita, jotka mahdollistavat palvelimien toimivuuden parantamisen. Virtuaalikoneiden avulla asiakasyritykset pystyvät käyttämään yhdellä fyysisellä koneella useita eri palveluita. Esimerkiksi tietyt ohjelmistot saatavat toimia paremmin eri käyttöjärjestelmällä, mutta perinteiseen tietokoneeseen ei voi asentaa kuin yhden kerrallaan. Virtuaaliset koneet mahdollistavat useiden eri käyttöjärjestelmien käytön sekä eri asetuksien tekemisen. Tämän lisäksi virtuaalikoneiden käyttö auttaa ohjelmistojen testaamisessa, sillä virtuaaliympäristössä pystytään eristämään mahdolliset syntyvät ongelmat eivätkä ne vaikuta muihin tietokoneen toimintoihin. (Gupta ym., 2010)

2.3 Tekninen tietoturva

Pilvipalveluiden tietoturvaa voi parantaa usein eri tavoin ja suurin osa turvallisuusmetodeista on samanlaisia muissakin tietojärjestelmissä. Pilvipalveluissa on kuitenkin uniikki ongelma tiedon suojaamisen kannalta, sillä eri toimijoita, joilla on pääsy pilvessä oleviin tietoihin, on valtavasti. Tieto tulisi olla salattua, jotta vaikka sen saisi haltuunsa joku ihminen kenelle se ei kuulu, niin sitä ei pystytä avaamaan tai lukemaan. (Ryan, 2013)

Normaali tiedon salaus ei kuitenkaan toimi pilvipalveluissa, sillä se estää palveluntarjoajaa käsittelemästä tietoa, mikä vuorostaan estää pilvipalvelun toiminnan muuttaen sen vain tallennustilaksi. Homomorfinen salaaminen kuitenkin poistaa tämän ongelman, sillä salatun tiedon pystyy avaamaan vain salausavaimella, joka tulkitsee salatun tiedon. Salausavain on algoritmin luoma satunnainen koodi. Tietoa voi siis siirtää verkon välityksellä turvallisesti, niin kauan kunhan salausavain pysyy määrättyjen toimijoiden hallussa. (Ryan, 2013)

Kyseessä ei kuitenkaan ole täydellinen metodi, sillä homomorfinen salaus vaatii käyttäjältä usein toimia ja on siitä johtuen tehoton. Esimerkiksi homorfisen salauksen avulla pystytään tekemään sähköpostin roskaposti-filtteri, joka tunnistaa roskapostin mutta ei osaa itse poistaa sitä. Sama periaate pätee pilvipalveluihin, pilvi osaa kyllä lukea salattua tietoa, mutta ei pysty toimimaan sen perusteella ilman käyttäjän toimia. Toinen rajoite liittyy salauksen raskaaseen toimivuuteen, salauksen purkamiseen vaaditaan tietokoneilta korkeaa laskentatehoa ja salatut tiedostot ovat usein eritäin suuria, mikä hidastaa toimintaa sekä vaikeuttaa toimintojen skaalattavuutta. (Ryan, 2013, Henry & Ali, 2017)

Toinen lähestymistapa olisi salata tieto ennen sen siirtämistä pilvipalveluun, minkä jälkeen tietoja pystyisi lukemaan vain salausavaimella. Tämä toimintatapa sopii parhaiten selaimen välityksellä tapahtuviin toimintoihin, sillä se rajoittaa pilven toimintaa. Lähestymistä voisi kuitenkin hyödyntää tiedon tallentamiseen sekä eteenpäin jakamiseen, kuten vaikka tietokantojen ylläpidossa. Esimerkiksi työnhakijoiden tiedot salattaisiin siinä vaiheessa, kun hakija ne syöttää selaimeen ja rekrytoija pystyisi ne hakemaan tietokannasta sekä käsittelemään niitä salausavaimen avulla. Tietoja ei kuitenkaan pystyisi selaamaan kuka vain, vaikka pääsisikin tietokantaan sisälle. (Ryan, 2013

On myös mahdollista, että tiedon salaus sidotaan tiettyyn ohjelmistoon, mutta se vaatii palveluntarjoajalta erityisjärjestelyjä. Käytännössä tämä lähestymistapa toimii niin että palveluntarjoaja omistaa salatuille salausavaimille tarkoitetun tallennustilan ja niitä voidaan käyttää vain tietyn ohjelman kautta. Tämä ohjelma on kehitetty yhdessä asiakasyrityksen kanssa. Asiakasyritys lataa salausavaimen pilvipalveluun, joka on sidottu pelkästään tähän ohjelmaan ja salausavaimella salattuihin tietoihin. Pilvipalvelu siis käyttää ohjelmistoa, joka pystyy käyttämään pilveen ladattua salausavainta tiedostojen lukemiseen. Tiedostoja ei kuitenkaan pysty lukemaan muilla

ohjelmistoilla. Tämän tiedonsuojaus metodin käyttöönotto on kuitenkin hankalaa (Ryan, 2013)

Kumar, Lakshmi, & Balamurugan (2015) esittelevät salausmetodin, joka perustuu tiedon attribuuttien salaamiseen. Vaikka salatut tiedostot vuotaisivat pilvipalvelusta, ei tiedostoissa olisi mitään hyödyllistä muille kuin tiedon omistajalle. Tämän metodin etuihin lukeutuvat tiedon helppo sekä halpa salaus, minkä lisäksi metodi on tehokas verrattuna muihin vastaaviin. Verrattuna esimerkiksi homomorfiseen salaukseen kyseessä on hinta-laatusuhteeltaan huomattavasti parempi vaihtoehto. Attribuuttien salaukseen perustuva toimintatapa on myös helposti skaalattavissa ja se on yleisessä käytössä useissa pilvipalveluihin liittyvissä tietoturvaratkaisuissa.

2.3.1 Virtuaaliset tietoturvaratkaisut

Tietoturvassa on useita eri näkökulmia ja yksi niistä on täysin virtuaalinen lähestymistapa. Nämä tietoturvaratkaisut perustuvat täysin virtuaalisten koneiden sisällä toimiviin protokolliin. Gary Anthes (2010) esittelee tekstissään useita eri tietoturvaratkaisuja alan suurimmilta kehittäjiltä, joita ovat Hewlett-Packard, IBM ja Microsoft. Hewlett-Packard on suunnitellut Solu Palveluna prototyyppiä, joka automatisoisi pilvipalveluiden tietoturvan. Solut olisivat yhteydessä useisiin virtuaalisiin koneisiin ja verkkoihin, jotka toimivat fyysisillä koneilla. Näiden solujen ympärille asennettaisiin sensoreita ja tunnistimia, jotka etsivät viruksia tai muuta luvatonta toimintaa. Sensorit voivat seurata suorittimien, muistin sekä sisään ja ulos kulkevan datan toimintaa, joita ne analysoivat perustuen vanhoihin käytösmalleihin tunnistaen luvatonta toimintaa. Solut voisivat jopa kopioida ja siirtää virtuaalisen koneen eri ympäristöön tarkempaa tutkintaa varten.

Toisaalta IBM kehitti prototyypin suojatusta virtuaalisesta koneesta, joka on samalla fyysisellä koneella, jossa muut palveluntarjoajan asiakkaiden virtuaalikoneet ovat. Prototyyppi pystyi seuraamaan asiakkaiden virtuaalisia koneita ja etsimään haitallista toimintaa. Lisäksi sen avulla kaikki asiakkaiden virtuaaliset koneet pystytään suojaamaan yhdellä viruksentorjuntaohjelmalla. Prototyyppi pystyi myös syöttämään pienen ohjelmiston asiakkaan virtuaaliseen koneeseen ja verrata sen näkemiä tiedostoja asiakkaan tiedostoihin, minkä avulla se pystyi selvittämään, onko virtuaalinen kone asiakkaan käytössä vai onko siihen asennettu haittaohjelmisto. Tulee kuitenkin huomioida, että virtuaalisiin koneisiin soluttautumista voitaisiin käyttää myös haitallisiin tarkoituksiin. Tästä johtuen asiakasyritysten tulisi aina pyytää, että heidän virtuaaliset koneensa sijaitsevat heille omistetuilla koneilla. Tämä ei kuitenkaan käytännössä välttämättä ole mahdollista, sillä ylläpitokustannukset kasvaisivat kohtuuttomiksi. (Anthes, 2010)

2.3.2 Tiedon käyttö ja saatavuus

Iso osa pilvipalveluiden tietoturvaa on tiedon käytön sekä pilven käyttäjien käyttöoikeuksien seuraaminen. Jotta pilvipalvelu olisi turvallinen, on ensisijaisen tärkeää estää luvaton pääsy, mutta samalla tulisi myös seurata luvallisten käyttäjien tiedon käsittelyä. Tämä onnistuu käyttäjien yksilöimisellä sekä henkilöllisyyden todentamisella.

Pilvipalveluiden todentamisessa ei kuitenkaan ole käytännöllistä tarkistaa fyysisiä henkilötodistuksia, joten todentaminen pitää suorittaa sähköisesti. Jotta sähköinen todentaminen olisi luotettavaa, käyttäjille tulisi määrittää sähköiset allekirjoitukset. Sähköisten allekirjoitusten teknologia perustuu pitkälti salausteknologiaan, jossa luodaan salattu avain, joka on sidottu käyttäjään ja näin pystytään varmistamaan käyttäjän oikeellisuus. Samalla pystytään seuraamaan millä avaimella tietoja on käsitelty pilvipalvelussa. Näin ehkäistään tiedon huolimatonta tai tahallisesti haitallista käsittelyä, kun jokaisen toiminnon pystyy jäljittämään tiettyyn käyttäjään. (Ardagna, Asal, Damiani & Vu, 2015)

Käyttöoikeuksien ja luvallisen pääsyn määrittelyyn on myös olemassa useita metodeja. Useat näistä perustuvat autoritaariseen järjestelmään, joka rajoittaa pääsyä eri avaintasojen avulla. Toisin sanoen asiakasyritykselle luodaan useita salausavaimia, joita ne voivat jakaa oman näkemyksensä mukaan. Avaimet on yleisimmin tehty attribuutteihin perustuvalla salauksella, sillä se on tehokasta ja halpaa. Toisaalta pilvipalveluiden käyttäjien todentamiseen ja erityisesti siirtyneen tiedon eheyden tarkistamiseen voidaan käyttää viestin todennus koodeja, jotka tarkistavat, ettei viestiä ole käsitellyt kukaan muu kuin lähettäjä ja vastaanottaja. (Ardagna ym., 2015)

3 ONGELMAT PILVIPALVELUIDEN TIETOTURVASSA

Tässä luvussa käsitellään pilvipalveluiden tietoturvauhkia sekä asioita, jotka vaikuttavat pilvipalvelun luotettavuuteen.

3.1 Luotettavuuden määrittely

Kaikkiin pilvipalveluihin kohdistuu uhkia tietoturvan kannalta, mutta on myös tärkeää selvittää palveluntarjoajan taustat, esimerkiksi se miten palveluntarjoaja käsittelee tietoja sekä kuka muu on vastuussa palvelun toiminnasta. (Neumann, 2014) Jos palveluntarjoaja tai muu palvelusta vastaava yritys menee konkurssiin, yrityksen tiedot voivat kadota.

Yksi suurimmista haasteista pilvipalveluiden levinneisyyden ja käytettävyyden laajentamisessa on tiedonhallinnan luotettavuus. On vaikea määritellä kaiken kattavia standardeja pilvipalvelujen luotettavuudelle, sillä tarjotut palvelut pohjautuvat yksityisiin pilviin, jotka ovat usein eri tavoilla toteutettu. Näin ollen ei voida asettaa automaattisia määreitä, jotka kaikkien pilvipalveluiden tulisi kohdata. Toisaalta useat kansainväliset organisaatiot, kuten ISO eli International Organization of Standardization, ovat määritelleet ”hyviä toimintatapoja” ja sääntöjä, mutta käytännössä palveluntarjoajalla ei ole mitään velvoitteita noudattaa niitä. Lisäksi asiakkaan on vaikea tiedostaa, milloin yrityksen tiedot on turvattu tai miten tietoturvaratkaisut on toteutettu. (Jaatun, Pearson, Gittler, Leenes & Niezen, 2016) Toisaalta ”hyvien käytänteiden” tarkoitus on olla yleispäteviä sekä jo hyväksi havaittuja, mutta ne eivät ota huomioon yritysten yksilöllistä kontekstia. (Siponen & Willison, 2009) Myös yritykset, jotka käyttävät näitä käytänteitä, saattavat saada niistä valheellista turvallisuuden tunnetta. Usein ajattelu voi kääntyä siihen, että tietoturva on nyt kunnossa, kun on seurattu standardeja, mutta todellisuudessa ei olla huomioitu tietoturvaa yrityksen omassa ympäristössä vaan vain toteutettu hyväksi todettuja käytänteitä.

(Siponen, 2006) Tämän lisäksi tiedon käsittelyn vastuu siirtyy palveluntarjoajalle, mutta samalla mikään ei estä kyseistä tahoa käyttämästä tietoa mielivaltaisesti. (Shahzad, 2014) Asiakkaan asema on teoriassa huono, koska alalla ei ole selviä standardeja, mutta pilvipalveluiden tietoturvaa tutkitaan jatkuvasti ja samalla myös syntyy uusia ratkaisuja.

3.2 Infrastruktuuri ja datanhallinta

Infrastruktuurilla tässä kontekstissa viitataan datakeskuksiin, joissa palveluntarjoajat tallentavat tiedot, jotka asiakas lisää pilvipalveluun. Kyseessä on usein palveluntarjoajan vuokraamia tiloja, joissa on useita servereitä. Näistä datakeskuksista pääsee käsiksi kaikkiin pilvipalvelun käyttäjien tietoihin. Yrityksillä, jotka ostavat pilvipalvelun on harvoin tietoa siitä mihin heidän tietonsa on tallennettu, joten he eivät voi tietää onko dataa suojattu mitenkään. Tiedon fyysisen turvallisuuden suojeleminen ei ole halpaa, sillä siihen vaaditaan vartijoita sekä valvontakameroita. Palveluntarjoaja voi tarjota takuita tiedon suojauksesta, mutta tiedot voivat sijaita useassa eri kohteessa sekä useassa eri maassa. (Sristrava & Kumar, 2015) Tämän lisäksi tiedot kulkevat usein monen eri palveluntarjoajan kautta, joten on mahdotonta tietää, onko kaikki palveluntarjoajan alihankkijat yhtä tarkkoja tiedon suojaamisen suhteen. Toisaalta jos palveluntarjoaja siirtää datakeskusta tai yhdistyy toisen yrityksen kanssa, tiedot voivat kadota tai jäädä käyttämättömille kovalevyille, vaikka asiakas olisi pyytänyt tiedon tuhoamista. (Shahzad, 2014) Pilvipalveluiden infrastruktuuriin liittyy paljon kysymyksiä, joita asiakasyritys ei välttämättä ymmärrä kysyä tai osaa edes tiedostaa uhkan mahdollisuutta.

Datanhallintaan sisältyy riski jo pelkästään tiedon valtavan määrän takia. Palveluntarjoajilla on useita asiakkaita, joilla on tuhansia tiedostoja, jotka tulisi pystyä erottelemaan sekä salaamaan, mutta samalla tietojen tulisi olla saatavilla nopeasti. Tämän lisäksi valtava määrä dataa on kultakaivos tiedon louhijoille, jotka hyödyntävät metadataa esimerkiksi markkinoinnin kohdentamisessa. Tästä johtuen useiden yritysten tietojenhallinta mahdollistaa rikollisen toiminnan lahjonnan sekä tietojen myynnin suhteen. (Ryan, 2011) Tiedon käsittelyyn liittyy myös inhimillinen tekijä, eli palveluntarjoajan tai asiakasyrityksen työntekijät, jotka usein aiheuttavat ongelmia, koska eivät ymmärrä täysin toimintansa seurauksia. Toisaalta myös vahinkoja tapahtuu aina kun ihminen on osallisena missä tahansa toiminnassa, esimerkiksi yksinkertaisen sähköpostin lähettäminen väärän osoitteeseen saattaa aiheuttaa valtavaa vahinkoa.

3.3 Saatavuus ja käyttöoikeudet

Pilvipalveluiden toimintamallin peruskivi on tiedon nopea sekä kattava saatavuus. Yrityksillä, jotka käyttävät pilvipalveluita, on yleensä useita työntekijöitä, joiden tulee pystyä käsittelemään samoja tiedostoja eri sijainneista. Tästä johtuen yrityksen tulisi pystyä luotettavasti tunnistamaan kuka pilvipalveluun pääsee sisälle sekä sen mitä tietoja on käsitelty. Yksinkertainen salasana tunnistus ei vielä takaa, että käyttöliittymää käsittelevät ainoastaan käyttöoikeuden saaneet työntekijät. (Ramachandran & Chang, 2016). Pilvipalveluiden lupaus siitä, että tietoa voi käsitellä missä vain ja millä tahansa laitteella luo valtavan haasteen käyttäjien tunnistamisessa. Perinteinen tiedon säilytys konttorissa tai tiedonkäsittely vain työpaikalla sijaitsevalla koneella luo fyysistä suojaa tiedolle, koska mahdollisen tietomurron tekijän tulisi myös murtautua yrityksen tiloihin. Pilvipalveluiden tapauksessa tietomurron voi tehdä etänä eikä tekijä tarvitse edes yrityksen omia laitteita. (Sristrava & Kumar, 2015) Toisaalta valtavien tunnistus- ja todennusprosessien käyttöönotto hidastaisi pilvipalveluiden käyttöä ja näin myös toimisi itse pilvipalvelun periaatteita vastaan.

Palvelunestohyökkäykset ovat yleistyneet internettiin yhdistettyjen laitteiden kasvun myötä. Palvelunestohyökkäyksessä rasitetaan palvelinta luomalla normaalista poikkeavaa liikennettä ja näin hidastetaan palvelimen toimintaa, mikä johtaa palvelun käytön hidastumiseen tai kaatumiseen. Liikenteen luomiseen käytetään usein suojaamattomia internettiin yhdistettyjä laitteita, mikä on työlästä perinteisin metodein, mutta pilven avulla hyökkäyksien tekeminen on helpompaa. Tämä johtuu siitä, että tekijöillä on nopea pääsy useisiin laitteisiin, jotka ovat yhteydessä toisiinsa pilven välityksellä. Hyökkäykset eivät rajoitu vain pilvipalveluihin, mutta voivat aiheuttaa pilvenkäyttäjille vakavia ongelmia. (Mirkovic & Reiher, 2004)

Pilvipalveluiden yleistymisen myötä on myös syntynyt uudenlainen tapa rikollisille hyödyntää palvelunestohyökkäyksiä. (Yan & Yu, 2015) Palvelunestosta aiheutuu välittömästi yritykselle ongelmia, koska pilvipalvelukäyttäjien liiketoiminta perustuu vahvasti tai kokonaan pilvessä olevaan tietoon. Kun tietoon ei pääse käsiksi, nykyisessä hektisessä liiketoiminnassa jokainen tunti saattaa maksaa yritykselle paljon. Toisaalta yrityksiä voidaan myös kiristää estämällä pääsy tietoihin. Tämän lisäksi, palvelunestohyökkäyksistä on kehittynyt uusi muoto pilvipalveluiden toimintamalliin perustuen. Uudenlainen hyökkäysmuoto, joka keskittyy palvelunkäyttäjän taloudellisen kestävyyden estämiseen tai heikentämiseen, on kohdennettu asiakkaisiin, jotka maksavat perustuen käytön määrään. Hyökkääjät luovat liikennettä, esimerkiksi yrityksen nettisivuille, jonka ylläpito perustuu pilvipalveluun, mikä näyttää normaaleilta kävijöiltä. Todellisuudessa liikenteen tarkoitus on aiheuttaa kuluja sivustoa ylläpitävälle yritykselle. (Yan & Yu, 2015) Toisaalta pilvien rajallinen kapasiteetti rajoittaa myös yritysten mahdollisuuksia toimia. Maailmanlaajuisten yritysten on mahdotonta siirtyä

täysin pilvipalveluiden varaan, sillä pelkät asiakastiedot saattaisivat kaataa palvelun.

3.4 Käyttäjien vastuu

Useat tutkimukset tietoturvallisuuden saralla ovat todenneet, että yksi suurimmista tietoturvauhkista ja vaikeasti hallittavista osista on käyttäjä. (Öğütçü, Testik, & Chouseinoglou, 2016, Paananen, Lapke & Siponen, 2020) Tämä johtuu jo pelkästään käyttäjien eli ihmisten luontaisesta taipumuksesta virheisiin. Toisaalta koneelle voi teoriassa kertoa mitä sen halutaan tekevän eikä se tee mitään muuta tai jätä mitään tekemättä. Ihmiselle voi kertoa ohjeet tai opettaa hänet tekemään joku tietty tehtävä, mutta se voi epäonnistua tai ohjeet unohtua.

Toisaalta tiedonkäsittelyä voidaan ohjeistaa kehittämällä tietoturvakäytänteitä ja julkaisemalla yrityksenlaajuiset ohjeistukset siitä, kuinka tietoa tulisi käsitellä. Ainakin teorian tasolla tämä on jo käytäntö useissa yrityksissä, mutta geneeriset käytänteet eivät välttämättä ole toimivia. Useissa tutkimuksissa on ilmennyt, että tietoturvakäytänteiden tulisi olla käytännönläheisiä ja olla relevantteja työntekijöiden jokapäiväisten työtehtävien kannalta. (Paananen, Lapke & Siponen, 2020) Ilman kontekstia tietoturvallisuus on helppo ohittaa vain taustaprosessina, joka huomioidaan vain silloin kun on jo tapahtunut vahinkoa. Käyttäjien toimintaa ohjaa agentti teorian mukaan omien hyötyjen maksimointi ainakin osin. Oletusarvoisesti siis käytöstä voi ohjata, mikäli siitä aiheutuu hyötyä käyttäjille. Perinteisesti ei-haluttua käytöstä on estetty pelottelemalla mahdollisilla seuraamuksilla (General deterrence theory). (Erickson & Gibbs, 1975) On kuitenkin mahdollista, että positiivisista toimista olisi tehokkaampaa palkita kuin rankaista toivomattomista teoista. Kehittämällä palkitsevaa järjestelmää voitaisiin ottaa ennakoivia askelia tietoturvan suhteen, eikä pelkästään reagoitaisi huonoon käytökseen. (Chen, Ramamurthy, & Wen, 2012) Oikeelliset toimet olisivat kuitenkin aina käyttäjien vastuulla, yritykset voivat vain yrittää ohjata käyttäjiä kohti oikeita valintoja.

Käyttäjällä on myös vastuu tiedosta, sillä pilvipalveluiden toiminta on vielä kehitysvaiheessa, eikä palveluiden toimintaan voi luottaa sokeasti. Tästä johtuen palveluiden käyttäjien tulisi tiedostaa riskit ja laittaa pilvipalveluihin vain tietoja, joiden vuotaminen ei ole kohtalokasta liiketoiminnalle. Toisaalta yrityksen johdon tulisi pitää huoli työntekijöiden työmoraalista sekä luotettavuudesta. Välinpitämättömät ja yritykseen sitoutumattomat työntekijät aiheuttavat tietoturvariskejä omalla käytöksellään. Vakavin uhka aiheutuu työntekijöiden omista ns. ”luvattomista” IT-ratkaisuista, joiden seuraamuksia ei välttämättä ymmärretä tai niistä ei välitetä. Lisäksi käyttäjillä on usein kova halu saada uusinta teknologiaa käyttöönsä, mutta unohdetaan, että niitä ei ole tutkittu tai testattu tarpeeksi, jotta voitaisiin todeta ne turvallisiksi. (Sristrava & Kumar, 2015) Pilvipalveluiden rakenteen takia, erityisesti PaaS-toimintamallissa,

käyttäjä pystyy lisäämään ohjelmistoja sekä muuntamaan sovelluksen asetuksia. Tästä johtuen ohjelmistoihin pystytään sisällyttämään haittaohjelmia, jotka saattavat vaarantaa koko palvelun toiminnan. (Tian, Lin & Ni, 2010) Toisin sanoen palvelua käyttävän yrityksen työntekijät pystyvät aiheuttamaan mittavaa vahinkoa omilla toimillaan tahallisesti tai tahattomasti.

4 LAINSÄÄDÄNTÖ JA SOPIMUKSET

Tässä luvussa käsitellään pilvipalveluihin kohdistuvia lakeja, säännöksiä sekä yritysten välisiä sopimuksia, jotka tukevat pilvipalveluiden ja yleisen tiedonkäsittelyn turvallisuutta.

4.1 Sopimukset ja lainsäädäntö

Pilvipalveluiden toimintaa on pyritty valvomaan useiden eri tahojen toimesta asettamalla lakeja, jotka luovat rajoitteita pilvipalveluiden tiedonkäytön suhteen. Nykypäivänä on kuitenkin helppo kiertää lakeja, koska ne ovat usein aluekohtaisia eivätkä samat säännöt päde esimerkiksi Yhdysvalloissa ja Euroopan Unionin maissa. Lisäksi palveluntarjoajat usein ulkoistavat datakeskukset ulkomaille, missä ylläpitokustannukset ovat alhaisemmat ja samalla ne siirtyvät kyseisen valtion lainsäädännön alaisiksi. Toisaalta jos yritys käyttää pilvipalvelua, jonka sijainti on Yhdysvalloissa, se siirtyy paikallisen Patriot Act :n alaisuuteen. Käytännössä Patriot Act on laki, joka antaa valtiolle oikeuden käyttää pilvipalvelusta löytyvää tietoa terrorinvastaisessa työssä sekä epäillyn Yhdysvaltoihin kohdistuvan vakoilun estämiseksi. (Sristrava & Kumar, 2015)

Ongelman ratkaisemiseksi tulisi kehittää yhteneväinen linja eri maiden välillä, missä apuna voitaisiin käyttää kansainvälisiä organisaatioita, jotka jo nyt edistävät eri maiden yhteistyötä. Esimerkiksi Yhdistyneet kansakunnat tai Maailman kauppajärjestö voisivat toimia johtavina tahoina pilvipalveluiden standardoimisessa. Näillä organisaatioilla on keinoja valvoa, että sääntöjä noudatetaan ja mahdollisesti rangaista rikkomuksista. (Narayanan, 2011)

Euroopan Unioni on laatinut tietosuojadirektiivin, joka kannustaa tiedon vapaaseen liikkuvuuteen Euroopan talousalueella yhdenmukaistamalla tietosuojakäytänteitä eri maiden välillä. Tiedon suojelu toteutetaan määräämällä tiedonkäsittelylle tiettyjä vaatimuksia, joiden laiminlyömisestä voidaan rangaista. Toisaalta direktiivi ei päde aina, jos maalla on omia

tiedonkäsittelyä koskevia lakeja ja rangaistukset vaihtelevat maakohtaisesti. (Hon, Hörnle & Millard, 2012)

Tietosuojadirektiiviin on tehty tarkennuksia sekä lisäyksiä vuosittain, sitä mukaa kun ala on kehittynyt ja levinnyt eri maihin. Euroopan Unionin kotisivuilla (2016a) kerrotaan sopimuksesta, jonka mukaan heinäkuussa 2016 Yhdysvallat ja Euroopan Unioni ottivat käyttöön Yksityisyydensuoja Kilpi nimellä olevan viitekehyksen. Se rajoittaa valtioiden pääsyä tietoihin, vahvistaa tietosuojakäytänteitä sekä määrää vuosittaisen tarkastustapaamisen, jossa varmistetaan käytänteiden toteutus. Tämän lisäksi EU on määritellyt perusteet riittävälle tiedonsuojaamiselle ja niiden perusteella listannut maat, jotka käsittelevät tietoa riittävän luotettavasti. Listalle pääseminen vaatii hyväksyntää muilta mailta, Euroopan komissiolta sekä Euroopan tietosuojavaltuutetulta. Toistaiseksi listalle on päässyt Euroopan ulkopuolisista maista : Andorra, Argentiina, Kanada, Färsaaret, Guernsey, Israel, Mansaaret, Jersey, Uusi-Seelanti, Sveitsi, Uruguay sekä Yhdysvallat. Listalla olevien maiden kautta voi turvallisesti siirtää tietoa ilman eri tietosuojatoimia. (Euroopan Unioni, 2016b)

Euroopan Unioni on kuitenkin perunut Yksityisyydensuoja kilpi (Privacy shield) sopimuksen Yhdysvaltojen kanssa vuonna 2020 Schrems II nimellä kulkevassa päätöksessään. Päätöksen perusteluna on, ettei amerikkalaiset yritykset ole pystyneet todistamaan, että ne tarjoavat GDPR:ssä määriteltyä tietoturvan tasoa. Päätös tuli voimaan heinäkuussa 2020, ja se siirsi vastuun tiedon turvallisesta siirrosta rekisterienpitäjille. Tässä tapauksessa siis julkisille organisaatioille, jotka keräävät ja tallentavat henkilötietoja pilvipohjaisiin palveluihin. Rekisterinpitäjien tulee siis huolehtia, että tietosuoja on riittävällä tasolla maassa, jossa tietoa säilytetään sekä tiedostaa maan lait (esim. patriot act Yhdysvalloissa) jotka mahdollistavat tiedon urkinnan. EU:n tavoitteena on kuitenkin kehittää uusi, paremmin henkilötietoja suojeleva sopimus Yhdysvaltojen kanssa, mutta sen aikataulusta ei ole tietoa. (Euroopan Unioni, 2020) Tämän sopimuksen purkamisen vaikutukset eivät vielä ole täysin nähtävissä, mutta tilanteeseen liittyy riskejä. Rekisterinpitäjän tulisi pystyä neuvottelemaan sopimukset uudestaan palveluntarjoajan kanssa sekä tekemään arvio palvelun tietoturvallisuudesta itsenäisesti. Tämä voi olla paitsi työlästä niin myös kallista, eikä rekisterinpitäjälle välttämättä jää mitään takuita turvallisuudesta. Ongelman suuruutta korostaa myös se, että suurimmat pilvipalveluiden tarjoajat sijaitsevat Yhdysvalloissa.

4.2 Turvallisuussertifikaatit ja tarkastukset

Pilvipalveluiden tarjonta on valtavaa, joten sopivan ja turvallisen palvelun valinta voi olla yrityksille vaikeaa eikä yrityksillä välttämättä ole resursseja tai tietotaitoa vertailla eri palveluntarjoajia. Tästä johtuen pilvipalveluiden vertailu tulisi järjestää ulkopuolisen yksityisen toimijan kautta, jotta markkinoille saataisiin näkemys siitä mitkä palvelut ovat turvallisia. (Singh, Jeong & Park,

2016) Palveluntarjoajan valinta on erityisen tärkeää, sillä palveluiden välillä vaihtaminen on hankalaa ja muutosten käyttöönotto kallista.

Sertifiointiprosessi on kuitenkin pitkä, sillä palveluntarjoajan toimintaa täytyy tarkastella perusteellisesti. Tämä johtuu siitä, että pilvipalveluiden tietoturvallisuuteen sekä toimivuuteen vaikuttavat useat asiat. Sertifikaatin vaatimuksissa tulisi olla tarkat laadulliset vaatimukset, kuten sopimusten ja lakiasioiden hoitaminen tietyin standardein, esimerkiksi palvelutasosopimuksien sekä tietosuojakäytäntöjen pakollisuus. Tämän lisäksi tarkastuksissa tulisi huomioida käyttöönottokäytännöt, tietojen salauksen toteutus sekä tiedon fyysinen suojaaminen datanhallintakeskuksissa. Toisaalta myös perinteiset liiketoimintakäytännöt, kuten laadunhallinta ja taloudelliset realiteetit, tulisi tarkastaa. Tämä on varsinkin manuaalisesti työlästä ja ostettuna työnä kallista. Accorsi, Lowis & Sato (2011) ehdottavat ratkaisuksi automaatiota, joka seuraa palvelun toimintaa ja tarkistaa, että tietyt parametrit täyttyvät. Tämä helpottaisi myös tarkastusten tekemistä, jos automaatio pystyttäisiin toteuttamaan luotettavasti. Tulee kuitenkin muistaa, ettei laatua voi käsitellä tässä kontekstissa subjektiivisesti, vaan standardien tulee syntyä tutkimuksen sekä käytännön testauksen kautta.

Sertifiointiin liittyy kuitenkin haasteita, jotka saattavat hidastaa innovaatiota ja vaikeuttaa markkinoiden toimintaa. Johtuen sertifiointiprosessin kustannuksista, sertifikaatin hankkiminen saattaisi olla mahdotonta pienemmille palveluntarjoajille ja näin asettaisi pienemmät yritykset huonompaan kilpailuasemaan markkinoilla. Lisäksi sertifikaattien valtavat vaatimukset saattavat nostaa pilvipalveluiden hintoja, koska yritysten pitää investoida sertifikaatteihin. Toisaalta sertifikaattien myöntämää laatutasoa tulisi tarkkailla sen myöntämisen jälkeen, sillä tarkastus takaa laadun vain sillä hetkellä. (Sunayev & Schneider, 2013)

Asiakasyrityksen kannalta on myös tärkeää, että pilvipalvelun tasoa pystytään seuraamaan ja että palveluntarjoajalla on vastuu tason ylläpidosta. Usein asiakkaan ja palveluntarjoajan välille tehdään palvelutasonsopimus, joka määrittelee asiakkaan vaatimukset palvelun suhteen, ja jos palvelu ei vastaa näihin vaatimuksiin, voidaan määrätä sanktioita. Palvelutasosopimukset ovat myös johtaneet teknologian ja toimintatapojen kehittymiseen, sillä palveluntarjoajat haluavat välttää mahdolliset sanktiot. (Lango, 2014)

4.3 Euroopan Unionin tietosuoja-asetus (GDPR)

Euroopan unionin tietosuoja-asetus vuodelta 2018 asetti yritykset sekä kaikki tietojen käsittelijät uuteen asemaan. GDPR on laki, joka suojaa EU:n kansalaisten tietoja kaikkialla maailmassa, joten ei ole väliä sijaitseeko tietojen käsittelijä Euroopassa. Lain noudattamisesta on vastuussa EU:n jäsenvaltiot ja rangaistukset vaihtelevat sakoista, jotka voivat olla kymmeniä miljoonia, aina tiedonkäsittelyn kieltämiseen artiklan 83(5) mukaan. (GDPR, (2018), s.83) Laki viittaa siis kaikkeen henkilökohtaisen tiedonkäsittelyyn, eikä siten rajoitu vain

julkiselle sektorille tai pilvipalveluihin. Tulee kuitenkin ottaa huomioon, että kaupungit ja kunnat edustavat valtiota ja siten ovat tarkemman valvonnan alla. Tämän lisäksi pilvipalveluiden tiedot voivat sijaita ympäri maailmaa, joten se asettaa uniikin näkökulman tietosuoja-asetuksen mukaiselle tiedonkäsittelylle.

4.3.1 Henkilökohtaiset tiedot ja niiden käsittely

GPDR määrittelee henkilötiedot artiklassa 4(1) tunnistetun tai tunnistettavan luonnolliseen henkilöön liitettävät tiedot, joiden avulla henkilö voidaan tunnistaa. Tähän sisältyy nimi, henkilötunnus, sijaintitiedot, verkkotunnistetiedot. Tämän lisäksi yksi tai useampi tunnistettava fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä lasketaan henkilötiedoksi. (GDPR, 2018, s.33) Kyseessä on siis erittäin laaja käsite, joka jättää varaa tulkinnalle, mikä vaikeuttaa lain toteutumista. Toisaalta tulisi myös huomioida, että data on yhdistettävä ”luonnolliseen henkilöön”, eli esimerkiksi henkilön omistaman yrityksen tiedot eivät ole lainsuojan alla. Mikäli tiedot jostain syystä vuotavat, on yrityksillä 72 tuntia aikaa ilmoittaa asiasta valvoville viranomaisille.

Kaupunkien ja kuntien kohdalla ei tarvita erillistä suostumusta tietojen käyttämiseen, toisin kuin yksityisellä puolella. Kaupunkien ja kuntien oikeus tietojen käyttöön perustuu artiklaan 6(1e), sillä ne toteuttavat yleistä etua koskevia tehtäviä ja/tai käyttävät julkista valtaa (GDPR, 2018, s.36). Pilvipalveluissa olevan tiedon laajan saatavuuden sekä nopean jakamisen takia henkilötietoja voi päätyä tarpeettoman tarkastelun alaiseksi ja/tai unohtua pilveen tarpeettomasti. GDPR:n artikla 5(1) toteaa, että henkilötietoja tulee käsitellä seuraavien periaatteiden mukaisesti: lainmukaisesti, kohtuullisesti, läpinäkyvästi, tarkoituksenmukaisesti, täsmällisesti sekä minimoiden (GDPR, 2018, s.35). Erityisesti pilvipalveluissa tiedon minimointi sekä tarkoituksenmukainen tarkastelu voi unohtua, kun tietoja ei käsitellä omalla koneella. Tiedon poistaminen tai minimointi voi usein unohtua, ellei sitä varten ole sovittu ajoitettuja tarkastuksia. Georgiopoulou, Makri, & Lambrinoudakis (2020) painottavat, että tietoa tulisi säilyttää vain hetkellisesti ja datan oikeellisuutta sekä tarpeellisuutta tulisi tarkistaa ennalta määritetyn aikataulun mukaisesti. Tämän lisäksi tietoa käsitelleiden henkilöiden oikeellisuus tulisi tarkistaa aika ajoin.

Toisaalta myös GDPR:n 5:n sekä 30:n artiklan mukaan tiedon käsittelyistä sekä käsittelijöistä tulee pitää kirjaa ja tarvittaessa ne tulee luovuttaa viranomaisille. Kirjanpidosta tulee selvitä rekisterinpitäjä, rekisterinpitäjän edustaja sekä tietoturvavastaavan nimi ja yhteystiedot. Lisäksi tulee kirjata tarkoitukset, kuvaus käsitellyistä ryhmistä, suunniteltu poistaminen sekä kenelle tietoja on luovutettu (kolmannet osapuolet). (GDPR, 2018, s.38)

4.3.2 Rangaistukset

GDPR:n säännösten rikkomisesta tulee usein vakavia seuraamuksia, mutta jokainen tapaus käydään läpi erikseen ja rangaistuksen tulee olla ”tehokasta, oikeasuhteista ja varoittavaa” (GDPR, 2018, s.82). Valvovat viranomaiset voivat estää tiedonkäsittelyn kokonaan tai määrätä hallinnollisia sakkoja, joiden suuruus vaihtelee tapauskohtaisesti, mutta korkeimmillaan ne voivat olla 20 miljoonaa euroa tai 4% edeltävän vuoden maailmanlaajuisesta liikevaihdosta. Toisaalta valtiot voivat soveltaa myös omaa rikoslakia tapauksissa, jossa se nähdään tarpeelliseksi. (GDPR, 2018)

Rikkomuksissa huomioidaan vakavuus, luonne sekä kesto. Tämän lisäksi arvioidaan, kuinka suureen joukkoon rikkomus on vaikuttanut ja millaiset vahingot se on aiheuttanut. Tämän lisäksi huomioidaan rikkeen tahallisuus, vastuu, aiempi rikehistoria, yhteistyö viranomaisten kanssa sekä onko aiempia toimenpidemääräyksiä noudatettu. (GDPR, 2018)

4.4 Suomen valtion pilvipalvelu linjaukset

Keskeisessä roolissa Suomen valtion linjauksissa on Valtiovarainministeriön julkaisema Julkisen hallinnon pilvipalvelulinjaukset (2018), joka on julkaistu ohjaamaan julkisten organisaatioiden omistaman tiedon käsittelyä pilvipalveluissa. Linjaukset kannustavat pilvipalveluiden käyttöön, mutta kuitenkin kehottavat käyttämään harkintaa siinä minkä palvelun ja keneltä sen hankkii, kuten minkä tahansa ICT-palvelun kohdalla. Valtionvarainministeriön työryhmä toteaa, että pilvipalveluita tulisi jopa suosia, mikäli ne tarjoavat parhaan ratkaisun eikä muita esteitä ole. (Valtiovarainministeriö, 2018)

Valtiovarainministeriön mukaan tiedon käsittelyssä tulee huomioida paitsi luottamuksellisuus, eheys sekä saatavuus, niin myös autentikointi sekä kiistämättömyys. Autentikointi tarkoittaa käyttäjän sekä palvelun identiteetin varmentamista, kun taas kiistämättömyys viittaa tiedon käsittelijän luotettavaan todentamiseen myös jälkikäteen. Tämän lisäksi tulee ottaa huomioon henkilötietojen käsittely GDPR:n vaatimusten mukaan. (Valtiovarainministeriö, 2018)

Vaikka pilvipalveluiden käyttöä jopa suositellaan, on niiden käytössä myös useita haasteita. Haasteiksi luetellaan: ei-julkisen tiedon käsittely, toiminnan jatkuvuuden takaaminen, tietoturvan ja -suojan toteutuminen tiedon sijainnista ja hallinnasta riippuen, riskienhallinnan moniulotteisuus sekä yksipuoliset sopimusehdot. Erityisesti toiminnan jatkuvuus on suuri riski, sillä jos pilvipalveluntarjoajan toiminta loppuu, voi tietojen saaminen olla vaikeaa tai jopa mahdotonta. Tämän lisäksi tietosuojan sekä tietoturvan toteutuminen on tärkeää taata. Riippuen siitä miten pilvipalvelu on toteutettu, tiedon fyysinen suojaaminen, esteetön kulku sekä tarvittaessa tuhoaminen tulee pystyä toteutumaan. Riskienhallinnan kannalta on tärkeää huomioida kuka

omistaa tiedon ja onko se aina saatavilla. Tämän lisäksi on harkittava voiko palveluntarjoaja käyttää tietoa kaupallisiin tarkoituksiin tai mikä on vastuu, jos tietoa katoaa. Toisaalta mitä tapahtuu tiedolle jos/kun toiminta loppuu. Myös sopimusehtoihin tulee paneutua tarkasti, jotta ymmärretään palvelun sekä tiedon käyttöoikeudet. Ei-julkisen tiedon tulisi olla aina saatavilla ja erityisesti kriittisen tiedon tulisi olla kaikissa olosuhteissa Suomessa saatavilla. (Valtiovarainministeriö, 2018) Valtiovarainministeriön linjaukset eivät varsinaisesti anna joka tilanteeseen sopivia ohjeita, vaan enemmän ohjenuoria, joita tulee soveltaa palveluita hankittaessa. Julkisilla organisaatioilla on erityinen vastuu tiedon turvallisen käsittelyn toteutumisessa, mutta monissa tilanteissa on jätetty paljon tulkinnan varaan.

Päätöksenteon tueksi on julkaistu myös Kyberturvallisuuskeskuksen toimesta Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri).). PiTuKrin tarkoituksena on helpottaa pilvipalveluiden turvallisuuden arviointia ja se on suunnattu erityisesti Suomessa toimivien viranomaisten käyttöön. Kriteeristön voi jakaa 11 pienempään osa-alueeseen sekä kahteen ylempään kategoriaan: Asiakkaan omat järjestelmät ja palveluntarjoajan järjestelmät.

1. Esiehdot
2. Turvallisuusjohtaminen
3. Henkilöstöturvallisuus
4. Fyysinen turvallisuus
5. Tietoliikenneturvallisuus
6. Identiteetin ja pääsyn hallinta
7. Tietojärjestelmäturvallisuus
8. Salaus
9. Käyttöturvallisuus
10. Siirrettävyys ja yhteensopivuus
11. Muutostenhallinta ja järjestelmäkehitys

- Kyberturvallisuus keskus, PiTuKri (2020)

Erityisen tärkeänä kohtana PiTuKri:ssa tulisi huomioida ensimmäinen osa-alue eli esitiedot. Tiedot palveluntarjoajasta, palvelusta, alihankkijoista sekä sopimusten sisällöt ovat ensisijaisen tärkeitä tietoturvan toteutumisen kannalta. Tämän lisäksi vastuualueet liittyen palvelun elinkaareen, turvallisuuteen sekä valvontaan tulisi olla selkeästi tiedossa. (Kyberturvallisuuskeskus, 2020) Tietoturvan toteutuminen on pitkälti ennakoiva prosessi ja sen takia juuri palvelun valintaan sekä sopimuksiin tulisi panostaa. Sopimuksien ehtoja voi olla vaikea myöhemmin muuttaa eikä virheitä välttämättä huomata ajoissa jälkikäteen. Tämän lisäksi tietomurroista tulevat kustannukset ovat usein huomattavat. IBM arvioi raportissaan vuonna 2020, että keskimääräinen kustannus tietomurrosta oli Yhdysvalloissa n. 3.9 miljoonaa dollaria. (IBM, 2020)

5 TUTKIMUSMENETELMÄ

Tässä luvussa käydään läpi empiirisen osion tutkimusmenetelmä sekä käydään läpi tutkimuksen tavoitteet. Tämän lisäksi luvussa esitellään empiiriselle tutkimukselle teoreettista taustaa ja lopuksi analysoidaan tutkimuksen tulokset.

5.1 Tutkimuksen tavoitteet

Tämän kyselytutkimuksen tavoitteena oli selvittää, minkälaisia käytänteitä julkisilla organisaatioilla on pilvipalveluiden käytön sekä hankinnan suhteen. Hankinta on sisällytetty kyselyyn, sillä sen ennakoiva vaikutus tietoturvan kannalta on merkittävä. Hankintaa edeltävät taustaselvitykset, riskianalyysit sekä kustannuslaskelmat vaikuttavat toiminnan jatkuvuuteen ja pienentävät riskejä pilvipalveluiden hankinnassa. Myös valtiovarainministeriön Julkisen hallinnon pilvipalvelulinjaukset (2018) painottaa linjauksissaan sopimusten sekä hankinnan aikana tapahtuvien prosessien merkitystä. Toisaalta johtuen EU:n Schrem II päätöksestä, sopimusten merkitys on vain kasvattanut merkitystään rekisterinpitäjien ja erityisesti julkisten organisaatioiden, jotka käsittelevät paljon henkilötietoja sekä muuta ei-julkista tietoa, toiminnassa.

Tavoitteisiin vastaamista varten kehittyi tutkimuskysymykseksi:

- *Millaisia käytänteitä julkisella sektorilla on pilvipalveluiden hankinnassa sekä käytössä*?

Tutkimuskysymykseen vastaamisen tavoitteena on selvittää, onko julkisilla organisaatioilla yhtenevät käytänteet pilvipalveluiden suhteen. Toisaalta tutkimuksen tarkoituksena on myös verrata vastauksia valtion linjauksiin sekä muihin rajoittaviin tekijöihin, jotta voidaan todeta, onko ohjeistuksella ollut toivottu vaikutus.

5.2 Teoreettinen tausta

Tutkimuksen taustalla on tiedon tallennuskapasiteetin tarpeen jatkuva kasvu sekä trendit, joiden mukaan tieto tulisi olla helposti sekä nopeasti saatavilla paikasta tai ajasta riippumatta. Pilvipalveluiden käyttö on yleistynyt valtavasti yrityspuolella, mutta sen tuomat riskit tiedonkäsittelyn saralla ovat aiheuttaneet ongelmia paitsi teknisestä näkökulmasta, niin myös käytänteiden kannalta julkisissa organisaatioissa. Tietoturvan tekniset ratkaisut riippuvat siitä, kuinka pilvipalvelu on toteutettu.

Euroopan Unioni teki vuonna 2012 aloitteen, jonka tarkoituksena oli ajaa eteenpäin yhtenäistä pilvipalvelustrategiaa EU valtioiden välillä erityisesti julkisissa organisaatioissa. Jo tuolloin on huomioitu pilvipalveluiden mahdolliset riskit. Aloitteessa on huomioitu erityisesti neljä eri kohtaa turvallisuuden parantamiseksi: teknologian standardointi, sertifikaattien kehitys, sopimusten kehittäminen sekä panostus eurooppalaiseen pilvipalvelu markkinaan sekä palveluntarjoajiin. (Euroopan Unioni, 2012) Siirtymä kohti pilvipalveluita on siis alkanut jo noin 10 vuotta sitten, mutta se on vielä pahasti kesken. Suurimmat pilvipalveluiden tarjoajat ovat Yhdysvalloista, mutta EU:n sisällä on kehitetty tietojenkäsittelylakeja sekä sertifiointeja tiedonkäsittelyyn. Toimet ovat kuitenkin ristiriidassa palveluntarjoajien sijainnin kanssa, sillä lait eivät ainakaan tällä hetkellä päde EU:n ulkopuolelle tallennettuihin tietoihin. Julkisilla organisaatioilla on myös vastuu palvella kaikkia kansalaisia yhdenvertaisesti, mikä osaltaan on voinut hidastaa pilvipalveluihin siirtymistä. Useat vanhempien ikäryhmien henkilöt tai ryhmät, joilla ei ole rahaa, eivät välttämättä pysty hoitamaan asioitaan sähköisesti. Toisaalta palveluiden tulee olla helppokäyttöisiä kaikille yhteiskunnan osapuolille, joten niiden suunnittelu voi olla hankalaa ja pahimmillaan ne voivat vahingoittaa ihmisten luottamusta valtion toimintaan. (Zaharia-Rădulescu & Radu, (2017).

Pilvipalveluiden toteutukseen on olemassa neljä vakiintunutta tapaa. Nämä ovat: oma konesali, yksityinen, hybridi sekä julkinen pilvipalvelu. Yritys käytössä on useimmiten yksityinen tai hybridi toteutus pilvestä. Tietoturvan kannalta on merkittävää, onko pilvipalvelun tarjoaja luotettava ja minne tieto on tallennettu. Mikäli tieto on yrityksen omissa konesaleissa, riskit pienenevät. Toisaalta jos tieto on viranomaisten ylläpitämissä palveluissa, riskit ovat myös matalammat, jos verrataan yksityisiin palveluntarjoajiin. Myös yksityisten palveluntarjoajien sijainnilla on merkitystä. Mikäli tietoa säilytetään Suomessa tai muualla EU:n sisällä, riskit ovat kohonneet mutta silti matalammat kuin EU:n ulkopuolella. (Valtiovarainministeriö, 2018) Erityisesti vuoden 2020 Schrems II päätös on nostanut riskien tasoa rekisterinpitäjille ulkomaisten palveluntarjoajien suhteen.

5.3 Tutkimusmenetelmä

Tämän tutkielman tutkimusmenetelmänä on strukturoitu kyselytutkimus, joka oli ohjattu julkisten organisaatioiden tietohallinnolle Suomessa. Tutkimus piti sisällään 30 kysymystä liittyen julkisten organisaatioiden käytänteisiin pilvipalveluiden hankinnassa sekä käytössä. Kysymykset pohjautuivat valtiovarainministeriön vuonna 2018 julkaisemaan Julkisen hallinnon pilvipalvelulinjaukset -dokumenttiin, jota käytetään myös vertailupohjana kyselytutkimuksen vastauksille. Valtiovarainministeriön (2018) linjaukset oli jaettu seitsemään eri kohtaan:

1. Pilvipalvelu hankintoja tulee käsitellä kuten muitakin ICT hankintoja.
2. Sopimukset, jatkuvuus sekä saatavuus vaativat erityishuomiota.
3. Hyöty sekä takuuvaatimukset tulee täyttyä hankinnassa.
4. Pilvipalveluita tulisi suosia, mikäli niiden hankinnalle ei ole esteitä ja ne tarjoavat parhaan hyödyn.
5. Hyödyn määrää sekä takuun toteutumista tulee seurata säännöllisesti.
6. Julkisen tiedon käsittelyä ei ole tarpeellista rajata.
7. Ei-julkista tietoa voidaan käsitellä julkisessa pilvipalvelussa, jos palvelun tietoturva ja tietosuoja on kunnossa.

Tulee kuitenkin muistaa, etteivät nämä linjaukset velvoita organisaatioita toimimaan niiden puitteissa, vaan niiden on tarkoituksena toimia ohjeistuksena. Nämä käytänteet kuitenkin sopivat vertailupohjaksi kyselyn vastauksille, sillä ne on jo todettu hyviksi tutkimuksen kautta valtiovarainministeriön toimesta.

Strukturoitu kyselytutkimus valikoitui tutkimusmenetelmäksi, koska se antaa mahdollisuuden kerätä dataa helposti ja usealta henkilöltä samalla säilyttäen tieteellisen eheyden. Menetelmän haasteena on usein se, että vastaukset ja sitä myöten tulokset perustuvat vastaajien kokemuksiin. (Snook & Harrison, 2001) Tämän tutkimuksen kannalta menetelmä on kuitenkin toimiva, sillä vastaajat on valittu nimenomaan heillä olevan kokemuksen vuoksi. Toisaalta tutkimuksessa myös määritellään alan tämänhetkistä tilannetta käytänteiden suhteen, joten kokemusten arvo korostuu.

Haasteita tämän menetelmän käytössä on myös tuloksiin vaikuttavat tekijät. Usein kysymysten asettelulla voi olla vaikutusta siihen, kuinka tutkimuksen kohteet vastaavat. Tämän lisäksi tuloksia voi myös vääristää väärinymmärrykset, tietämättömyys, mielipiteen esittäminen faktana sekä arvailu. (Snook & Harrison, 2001) Näitä haasteita on koitettu minimoida asettelemalla kysymykset niin, ettei niillä ole useita tulkintatapoja. Toisaalta kysely on toteutettu anonyyminä, jotta väärien vastauksien pelko ja sen myötä arvailun kasvaminen pystytään minimoimaan. Kysymykset ovat myös kaikille samat, jotta vastaukset ovat vertailukelpoisia. Tämän lisäksi kysely on yritetty pitää kohtuullisen pituisena, ettei siihen vastaaminen olisi liian työlästä ja näin vastauksien määrä laskisi.

5.4 Datan kerääminen

Tämän tutkimuksen kysely on toteutettu käyttäen Likertin asteikkoa, joka mittaa vastaajien asenteita esitettyihin väittämiin. Likertin asteikko on laajasti hyväksytty tieteellinen metodi ja se on kehitetty jo vuonna 1932. Likertin asteikko auttaa tulosten analysoinnissa, muuttaen ihmisten käsitykset ja mielipiteet enemmän kvantitatiiviseen muotoon. (Joshi, Kale, Chandel, & Pal, 2015) Tässä tutkimuksessa käytettiin asteikkoa 1–5, jossa 1 tarkoittaa että vastaaja on täysin erimieltä, kun taas 5 tarkoittaa että vastaaja on täysin samaa mieltä väitteen kanssa. Asteikon keskellä oleva arvo 3 tarkoittaa, ettei vastaaja tiedä tai hänellä ei ole mielipidettä väittämään.

Tutkimuksen datan keräämisen aikana ilmeni useita haasteita saada vastauksia kyselyyn. Kyselyn alkuperäinen kohdeyleisö oli tietosuojavastaavat, mikä kuitenkin nopeasti siirtyi julkisten organisaatioiden tietohallinnon puoleen. Kyselyä varten kontaktoitiin useita henkilöitä puhelimitse sekä sähköpostitse ja ensimmäiset reaktiot olivat usein positiivisia, mikä korosti aiheen tärkeyttä. Vastauksia kyselyyn ei kuitenkaan juurikaan kertynyt ja kyselyn kohdeyleisöä laajennettiin ottamalla yhteys Kuntaliittoon, jonka viestinnän piirissä oli suuria määriä kaupunkien tietohallintohenkilökuntaa. Läheskään kaikissa suomalaisissa julkisissa organisaatioissa ei ole vielä siirrytty pilvipohjaisiin palveluihin tai siirtymä on vielä kesken.

Kohdeyleisön matala vastausaste voi johtua kyselyn väärästä kohdentamisesta, mikä myös tuli ilmi alkuperäisten kontaktointien kautta. Tähän kuitenkin reagoitiin ja kyselyn kohdetta tarkennettiin sekä kyselyn kontaktointeja laajennettiin. Kyselyä on myös katsottu kontaktointien määrän nähden hyvin vähän, mikä selittyy osaltaan sillä, että kysymykset toimitettiin myös PDF muodossa. Ongelma on siis mahdollisesti kyselyn rakenteessa tai kysymyksissä. Kyselystä ei ole tullut suoraa palautetta, mutta vastausinnon laantuminen ensi kontaktista kyselyn toimitukseen herättää ihmetystä.

6 TULOKSET

Tässä luvussa esitellään empiirisen tutkimuksen tulokset sekä analysoidaan niiden merkitystä.

6.1 Tulokset

Tämä tutkimus toteutettiin alalta nousseen tarpeen takia selventää käytänteitä pilvipalveluiden osalta julkisissa organisaatioissa. Hypoteesina toimi, ettei alalla ole juurikaan yhteneviä käytänteitä ja että jokaisella organisaatiolla oli omat tavat hyödyntää pilvipalveluita. Tutkimuksen tarkoituksena ei ollut selventää hyviä käytänteitä, vaan luoda katsaus alalla vallitsevaan tilaan. Tämän myötä tuloksia on vaikea yleistää niiden luonteen puolesta, mutta myöskään määrän puolesta.

Empiirisen tutkimuksen tulokset olivat suppeat laajasta kontaktoinnista sekä vastaajien kanssa käydyissä keskusteluissa ilmenneestä kiinnostuksesta huolimatta. Kyselyyn vastasi vain 5 ihmistä vaikka kyselyä varten kontaktoitiin useita kymmeniä ihmisiä puhelimitse sekä sähköpostin välityksellä. Vastaukset ovat hajautuneet, mikä osaltaan osoittaa julkisten organisaatioiden pilvipalvelukäytänteiden hajaantuneisuutta. Taulukossa 1 esitellään kyselyn vastauksien jakauma, jossa vasemmalla kysymys ja oikealla asteikko 1–5 missä 1 tarkoittaa täysin eri mieltä ja 5 täysin samaa mieltä. Laatikoihin on merkitty miten monta vastaajaa vastasi tietyllä tavalla kyseiseen kysymykseen.

Tulosten osalta on myös hyvä huomioida erityisesti julkisten organisaatioiden erivaiheiset siirtymät pilvipalveluiden käyttöön ja niiden eri käyttöasteet. Tämän lisäksi kyselyssä oli useita kysymyksiä liittyen sopimuksiin sekä palveluiden hankintaan, mutta vastaajat eivät välttämättä ole olleet osana hankinta- ja sopimusprosessia. Sopimusten sisältö ei siis välttämättä ole tuoreessa muistissa.

TAULUKKO 1 Kyselytutkimuksen tulokset

Kysymys	Vastausten määrä				
	1	2	3	4	5
1. Pilvipalveluiden hankinnassa otettiin huomioon alan trendit?				4	1
2. Pilvipalveluiden hankinnassa mietittiin myös vaihtoehtoisia toteutuksia?		1	2	1	1
3. Pilvipalveluiden hankinnassa huomioitiin riskit ja kartoitettiin markkinoita?		1	2	2	
4. Palveluntarjoajan tausta ja tulevaisuus otettiin huomioon valinnassa?		1	1	2	1
5. Palveluntarjoajan kanssa neuvoteltiin mahdollisista muista palveluista?		2	1	2	
6. Palvelusopimuksiin on kirjattu vastuualueet?			1	3	1
7. Sopimus on kirjattu kielellä jonka kaikki osapuolet ymmärtää?		1	1	3	
8. Sopimuksiin on kirjattu mitä tiedolle tapahtuu palveluntarjoajan lopettaessa?		1		4	
9. Sopimuksiin on kirjattu kuinka häiriötilanteet ratkaistaan ja niiden vastuualueet?		2	1	1	1
10. Sopimuksiin on kirjattu kuinka ja miten tieto saadaan siirrettyä palveluntarjoajan vaihtuessa?	2		2	1	
11. Sopimuksiin on kirjattu millä tasolla palvelun tason tulee olla?		1		4	
12. Sopimuksiin on kirjattu mahdollisesta palvelun kehittämisestä vastuut?		1	2	2	
13. Sopimuksiin on määritelty hyväksytyt kustannusten muutokset?		2	1	1	1

14. Sopimuksiin on määritelty palvelutakuu?		2	1	2	
15. Palvelun kapasiteetti, saatavuus sekä tietoturva on määritelty sopimuksessa?		1		3	1
16. Pilvipalveluihin kohdistuvat esteet/haasteet on otettu huomioon hankinnassa?		1	2	2	
17. Hankintaa edelti riski- ja kustannushyöty analyysi?	1	2	2		
18. Palveluiden elinkaari huomioitiin hankintaa tehdessä?	1		1	2	1
19. Palveluiden tasoa seurataan suunnitelmallisesti?		1	2	2	
20. Hankinnassa hyödynnettiin ulkopuolista riippumatonta konsulttia tai vastaavaa?		2	2	1	
21. Pilvipalveluissa tiedon käsittelyä seurataan ja ohjeistetaan?		1	3		1
22. Pilvipalveluissa poistetaan tietoa määräajoin?		2	3		
23. Henkilötietojen käsittelyä seurataan ja ohjeistetaan pilvipalveluissa?		3			2
24. Pilvipalveluihin ladattavaa tietoa rajoitetaan riippuen sen laadusta? (Julkista tietoa/ei-julkista tietoa)		2		2	1
25. Pääsyä pilvipalveluihin on rajattu tarpeellisuuden mukaan?			1	2	2
26. Tietomurron varalle on tehty suunnitelma, jossa määritellään vastuualueet?		2	1	2	
27. Pilvipohjaisissa pikaviestimissä jaettavaa tietoa on rajoitettu?		3			2
28. Pääsyä pilvipalveluiden eri osiin on rajattu tarpeen		1	1	1	2

mukaan?					
29. Pilvipalveluiden käyttämättömät tunnukset poistetaan heti?		1	2	2	
30. Pilvipalveluiden salasanat vaihdetaan tietyin määräajoin?			2	2	1

Tuloksista on huomattavan suurta hajontaa vastauksissa, mikä vaikeuttaa tuloksista yksiselitteisten ratkaisujen johtamista. Toisaalta osassa kysymyksissä on selkeämpää jakaumaa, kuten kysymyksessä 1. alan trendejä on selkeästi kartoitettu ennen hankintaa. Seuraavassa kappaleessa käydään vastauksia läpi tarkemmin ja kysymyksiä jaotellaan osa-alueisiin.

6.2 Tulosten analyysi

Tämän tutkimuksen tuloksiin olisi turha kohdentaa suuria tilastollisia menetelmiä sillä materiaalia on niin suppeasti. Tämä ei kuitenkaan tarkoita, etteikö tuloksista voisi johtaa päätelmiä. Kyselyn voi jakaa karkeasti kahteen osaan: hankintaan ja sopimuksiin liittyvät käytänteet sekä palveluiden käyttöön liittyvät käytänteet. Hankintaan ja sopimuksiin liittyvät käytänteet ovat selkeästi suuremmassa osassa, sillä noin 20 kysymystä liittyvät niihin. Kuten PiTuKri:ssakin todettiin, ennakoivat ratkaisut ovat erittäin isossa osassa tietoturvan takaamisessa. Tästä johtuen tulokset käsitellään kahdessa osassa, jotta vastauksia on helpompi verrata toisiinsa ja voidaan tehdä päätelmiä.

6.2.1 Sopimukset ja hankinta

Pilvipalveluiden hankinnassa tulisi harjoittaa erityistä varovaisuutta sillä riippuen ostetusta palvelusta, asiakas ei välttämättä pysty muuten tarkistamaan tai takaamaan tietoturvan tasoa, ellei sitä ole tehty etukäteen. Varsinkin SaaS toteutuksissa asiakas joutuu pitkälti luottamaan palveluntarjoajaan, että tietoturva on kunnossa. Tästä johtuen onkin ensisijaisen tärkeää valita palveluntarjoaja huolellisesti. Kyselyssä oli yhdeksän kysymystä, jotka liittyivät palveluntarjoajan valintaan / palvelun hankintaan.

TAULUKKO 2 Vastausprosentit hankintakysymyksiin.

Kysymys numero		Vastausprosentti					
	Täysin eri mieltä	1	2	3	4	5	Täysin samaa mieltä
1					80	20	
2			20	40	20	20	

3			20	40	40		
4			20	20	40	20	
5			40	20	40		
16			20	40	40		
17		20	40	40			
18		20		20	40	20	
20			40	40	20		

Taulukosta 2 selviää hankintaan liittyvien kysymyksien vastausprosentit. Osa kysymyksistä selkeästi jakoi enemmän vastaajien mielipiteitä kun osaan vastaukset olivat selkeästi yhtenäisemmät. Kysymyksessä 1. trendien huomioimisesta vastaajat olivat 100% samaa tai täysin samaa mieltä. Tämä osoittaa, että organisaatioissa on huomioitu jo EU:nkin ajama digitalisaatio ja siirtyminen kohti pilvipohjaisia ratkaisuja. Toisaalta kysymyksen 2. vaihtoehtoiset ratkaisut pilvipalveluille jakoi mielipiteitä, mutta suurin osa vastaajista totesi organisaatioiden joko harkinneen muita vaihtoehtoja tai eivät osanneet vastata.

Kysymyksestä 3. markkinoiden sekä riskien kartoittamisesta olivat suurin osa vastaajista sitä mieltä, että tämä on toteutunut hankinnassa. On kuitenkin mielenkiintoista, että vastaajat olivat eri mieltä kysymyksessä 17. riski- ja kustannushyöty analyysin tekemisestä. Kukaan vastaajista ei ollut tehnyt analyysiä ennen hankintaa, mutta koki, että riskit ja markkinat oli kuitenkin kartoitettu. Tämän lisäksi kysymyksessä 16. pilvipalveluiden esteiden ja haasteiden huomioimisesta 40% vastaajista oli selkeästi miettinyt palveluiden rajoitteita. Tässä käytänteessä on kyse pilvipalveluiden rajoitteiden ymmärtämisestä. Pilveen tallennettu tieto on nopeasti saatavilla ajasta ja paikasta huolimatta, mutta onko se samalla turvassa asiattomalta käsittelyltä tai katselulta.

Kysymyksen 4. palveluntarjoajan taustan ja tulevaisuuden huomioimisesta oli selkeästi 60% vastaajien näkökulmasta toteutunut. Tämä on tärkeä käytänne, sillä palvelun jatkuvuus on ensisijaisen tärkeää tiedon eheyden sekä turvallisen säilyttämisen kannalta. Kysymys 5. muiden palveluiden neuvotteluista jakoi vastaajien mielipiteet kahtia, 40% ei ollut neuvotellut muista palveluista palveluntarjoajan kanssa ja 40% oli niin tehnyt. Myös tämä käytänne on palveluiden jatkuvuuden sekä tiedon esteettömän kulun kannalta tärkeää, mutta ei kuitenkaan pakollista. Tämän lisäksi kysymys 18. liittyen palveluiden elinkaaren huomioimiseen on jatkuvuuden kannalta merkittävä. 60% vastaajista oli sitä mieltä, että elinkaari on huomioitu palveluita hankkiessa ja vain 20% oli sitä mieltä, että sitä ei oltu huomioitu.

Viimeinen kysymys (20.) hankintaan liittyen oli ulkopuolisen avun hankkimisesta. Vain yksi vastaajista oli hyödyntänyt ulkopuolista konsultaatiota, kun taas 40% vastaajista arvioi hankintaa vain itse. Ulkopuolisten konsulttien hyödyntäminen voi aiheuttaa ylimääräisiä kustannuksia hankintavaiheessa, mutta samalla auttaa varmistumaan palveluntarjoajan laadusta ja voi pitkässä juoksussa osoittautua

kustannustehokkaaksi. Palveluntarjoajia on valtava määrä eikä kaikilla yrityksillä välttämättä ole aikaa, varaa tai taitoa arvioida niiden tasoa.

Kuten hankintaan liittyvät kysymykset niin myös sopimustekniset kysymykset ovat ensisijaisen tärkeitä onnistuneen hankintaprosessin toteutumiseksi. Sopimuksilla on tarkoitus suojata asiakasta ja helpottaa palvelun tason seuraamista. Sopimuksiin liittyviä kysymyksiä oli kaiken kaikkiaan kymmenen.

TAULUKKO 3 Vastausprosentit sopimuskysymyksiin.

Kysymys numero		Vastausprosentti					
	Täysin eri mieltä	1	2	3	4	5	Täysin samaa mieltä
6				20	60	20	
7			20	20	60		
8			20		80		
9			40	20	20	20	
10		40		40	20		
11			20		80		
12			20	40	40		
13			40	20	20	20	
14			40	20	40		
15			20		60	20	

Taulukko 3. esittää vastausprosentit sopimuskysymyksiin, jotka ennakkoon oli arvioitu vaikeimmaksi vastata johtuen siitä, että sopimukset eivät välttämättä ole tuoreessa muistissa. Puhelinkontaktointien aikana ilmeni myös vastaajien toimesta, että sopimuksia tutkitaan vain, jos siihen ilmenee tarvetta. Sopimuksien merkitys on myös valtava asiakkaan aseman turvaamisessa, mutta isojen palveluntarjoajien kanssa voi olla vaikea neuvotella yksilöityjä sopimuksia.

Kysymys 6. vastuualueiden kirjaamisesta sopimuksiin sai vastaajilta yksimielisen vastauksen, sillä 80% vastaajista koki, että sopimuksiin oli kirjattu vastuualueet. Tämä on tärkeä käytänne ja sopimusten tulisikin sisältää myös mitättömiltä tuntuvien prosessien vastuut, jotta asiakkaan asema olisi mahdollisimman hyvä. Toisaalta kysymyksen 9. tarkemmin määritelty vastuun jako häiriötilanteissa sai 40% vastaajista toteamaan, ettei vastuita ole niin tarkkaan määritelty. Tämä vaikeuttaa häiriötilanteiden ratkaisua sekä hidastaa palvelun paluuta normaaliin. Kysymys 7. sopimusten kielestä saattaa tuntua ilmiselvältä ja 60% vastaajista myös koki sopimukset ymmärrettäviksi kun taas 20% mielestä näin ei ole. On kuitenkin tärkeää huomioida, että jos sopimus on käännetty toisesta kielestä toiselle, voi olla mahdollista, että käännöksessä hukkuu merkittävää tietoa.

Kysymyksessä 8. palvelussa olevan tiedon kohtalosta, mikäli palveluntarjoaja lopettaa olivat vastaajat 80% sitä mieltä, että tiedon takaisin saaminen on määritelty sopimuksessa. Tämä on myös jatkuvuuden kannalta tärkeää, sillä ilman määrittelyä tiedot saatetaan menettää. Kysymys 10 oli myös

suunnattu tiedon siirtoon palveluntarjoajalta, mutta tällä kertaa mikäli palveluntarjoaja vaihtuu. Vastaajista 40% koki, että palveluntarjoajan vaihtamisesta ei ole mainintaa sopimuksessa ja vain 20% koki, että sopimuksessa on määritelty tiedon kohtalo vaihdon tapahtuessa. Käytännössä ilman sopimusta tietojen siirto voi olla erittäin työlästä, sillä mikään ei velvoita palveluntarjoajaa helpottamaan prosessia.

Kysymykset 11–15 liittyivät kaikki jollain tavalla palvelun toimivuuteen, tasoon tai kustannuksiin. Kysymykseen 11. siitä onko sopimuksiin kirjattu palvelun taso, vastaajista 80% oli sitä mieltä, että hyväksyttävä taso on määritelty, kun taas 20% koki ettei näin ole. Palvelun tason määrittely on erittäin tärkeää, jotta asiakas voi seurata saako rahoilleen vastinetta. Kysymys 12. kehittämisen vastuista sopimuksissa jakoi vastaajien mielipiteitä. Vastaajista 40% koki, että kehittämisen vastuut on selkeästi jaettu, kun taas 20% mielestä näin ei ollut. Palveluiden kehittäminen on tärkeää paitsi tietoturvan kannalta, niin myös palvelun käytettävyyden kannalta. Ensisijainen vastuu palvelun kehittämisestä on tietenkin palveluntarjoajalla, mutta ilman merkintää siitä sopimuksissa palveluntarjoaja voi lopettaa tarjotun tuotteen kehittämisen ja myydä uuden kehittyneemmän tuotteen myöhemmin tilalle. Kysymys 13. liittyi kustannusten muutoksiin, ja myös tämä jakoi vastaajien mielipiteitä. Vastaajista 40% oli sitä mieltä, ettei kustannuksien muutoksista ole merkintää sopimuksissa ja 40% oli sitä mieltä, että hyväksytyt rajat on sovittu. Vaarana kustannusten muutoksissa on se, että ilman sopimuksia palveluntarjoaja voi sopimusteknisestä näkökulmasta muokata ylläpito- ja muita kustannuksia mielensä mukaan.

Kysymykseen 14. siitä sisältääkö sopimukset palvelutakuuta vastasi 40% vastaajista, ettei takuusta ole mainintaa sopimuksista, 40 % vastaajista ei osannut vastata kysymykseen tai ei ollut varma. Palvelutakuu on erittäin tärkeä osa tietoturvan toteutumista, sillä se määrittää millä tasolla palveluntarjoaja takaa palvelun toimivan ja kuinka nopeasti häiriötilanteiden jälkeen se palautuu normaaliksi. Onkin huolestuttavaa, jos julkisilla organisaatioilla ei ole sopimuksissaan merkintää palvelutakuusta. Kysymys 15. palvelun kapasiteetista, saatavuudesta sekä tietoturvasta sai selkeän vastauksen kun 80% vastaajista koki, että näiden taso oli hyvin sopimuksissa merkitty. Toisaalta 20% vastaajista koki, ettei näin ole, mikä on myös huolestuttavaa julkisten organisaatioiden kannalta, jos jossain ei näin ole.

6.2.2 Palvelun käyttöön liittyvät käytänteet

Palveluiden käyttöön liittyviin käytänteisiin suunnatut kysymykset olivat vastaajille selkeimmät eli vastauksissa oli vähiten jakaumaa. Kysymyksiä kertyi yhteensä kymmenen eli suunnilleen sama määrä kuin muistakin aiheista, mutta niiden käytännönläheisyys varmasti auttoi vastaajia antamaan selkeitä

vastauksia. Teoriassa kysymyksiin pystyisi vastaamaan myös aivan normaali käyttäjä eivätkä ne varsinaisesti vaadi asiantuntijuutta.

TAULUKKO 4 Vastausprosentit käyttöön liittyvissä kysymyksissä.

Kysymys numero		Vastausprosentti					
	Täysin eri mieltä	1	2	3	4	5	Täysin samaa mieltä
19			20	40	40		
21			20	60		20	
22			40	60			
23			60			40	
24			40		40	20	
25				20	40	40	
26			40	20	40		
27			60			40	
28			20	20	20	40	
29			20	40	40		
30				40	40	20	

Taulukosta 4. näkee vastausprosentit pilvipalveluiden käyttöön liittyvissä kysymyksissä. Kysymykseen 19. seurataanko palveluiden tasoa aktiivisesti vastaajista 40% vastasi että seurataan, kun taas 20% oli sitä mieltä, ettei seurata ja 40% ei osannut vastata. Palveluntason seuraaminen olisi tärkeää, jotta asiakasyritykset eli tässä tapauksessa julkiset organisaatiot voisivat todentaa, että saavat rahoilleen vastinetta.

Kysymykseen 21. seurataanko sekä ohjeistetaanko tiedon käsittelyä pilvipalveluissa, 60% ei osannut vastata, kun taas 20% oli sitä mieltä, että seurataan ja 20% sitä mieltä että ei. Tiedon käsittelyn seuranta voi olla myös hyvin huomaamatonta, joten se voi joissain tapauksissa mennä ohi, mutta ottaen huomioon, että vastaajat olivat tietoturvan ammattilaisia niin en usko että siitä oli tässä kyse. Toisaalta kysymykseen 23. seurataanko henkilötietojen käsittelyä 60% vastasi ei ja 40% kyllä. Henkilötiedot luokitellaan ei-julkiseksi tiedoksi, joten niiden käsittelyä tulisi ehdottomasti seurata tietoturvan toteutumisen kannalta. On myös huolestuttavaa, jos työntekijöitä ei ohjeisteta tiedonkäsittelyyn pilvipalveluissa, sillä se on huomattavan erilainen ympäristö kuin henkilökohtaiset koneet. Kysymykseen 24. rajoitetaanko tiedon lataamista pilvipalveluihin sen julkisuuden perusteella 40% vastasi ei ja 60% kyllä. Ei-julkisen tiedon säilyttäminen pilvipalveluissa ei ole kiellettyä, mutta sen tulisi sijaita yksityisessä pilvessä eikä missään vaiheessa joutua väärälle yleisölle. Toisaalta käyttäjien voi olla vaikea tietää ilman seurantaa, minne tietoa voi turvallisesti tallentaa. Kysymys 27. tiedon jakamisen rajoittamisesta pilvipohjaisissa pikaviestimissä sai vastaajilta 60% ei ja 40 % kyllä. Pilvipohjaisten pikaviestimien ongelma on, että keskustelut säilyvät pitkiä aikoja ja ne voidaan helposti jakaa usealle henkilölle. Muun muassa Teamsissä voi jakaa tiedostoja suoraan sharepointtiin tai lisätä henkilöitä keskusteluun ja jakaa keskusteluhistoria. Näin ollen tietoa saattaa päätyä asiattomille henkilöille,

vaikka keskustelu olisi alun perin ollut vain asianomaisten välinen. Onkin huolestuttavaa, jos käytäntönä ei ole rajata niissä jaettavaa tietoa.

Kysymykseen 22. poistetaanko tietoa tietyin määräajoin pilvipalveluista 40% vastasi että ei ja 60% ei osannut sanoa. Tiedon poistaminen tasaisin väliajoin olisi tärkeää, ettei turhaa tietoa kerry tai unohdu palveluihin, sillä tietoa tulisi säilyttää vain niin kauan kuin sitä tarvitaan. Sama periaate toimii vanhoihin tunnuksiin. Kysymykseen 29. poistetaanko käyttämättömät tunnukset heti vastasi 40% kyllä, kun taas vain 20% ei ja 40% ei osannut ottaa kantaa. Tunnuksien poistaminen on äärimmäisen tärkeää, jotta asiaton pääsy palveluihin estetään. Toisaalta myös tunnusten hallinnointiin liittyy vahvasti salasanojen vaihto. Tämä on myös yksi tietoturvan perustoimenpiteistä, mutta kysymykseen 30. vaihdetaanko salasanoja tietyin määräajoin vastattiin 60% kyllä ja 40% ei osannut ottaa kantaa. Se että vastausprosentti ei ole 100% on kyllä hieman huolestuttavaa julkisten organisaatioiden kannalta ottaen huomioon kuinka perustavanlaatuinen käytäntö on kyseessä.

Kysymykseen 25. onko pilvipalveluihin pääsyä rajattu tarpeellisuuden mukaan vastattiin 80% kyllä ja 20% ei osannut sanoa. Pääsyn rajaaminen on perustoimenpide tietoturvan kannalta ja on hyvä huomata, että myös julkiset organisaatiot ovat tämän toteuttaneet. Toisaalta kysymykseen 28. onko pilvipalveluiden eri osiin rajattu pääsy, vastattiin hyvin hajaantuneesti: 60% vastasi kyllä, 20% ei ja 20% ei osannut sanoa. Eri osioiden rajaaminen on tärkeää tietoturvan kannalta, jotta tietoja eri osioissa pääsee käsittelemään vain tietty osa käyttäjistä. Tämän myötä myös tiedon oikeellisen käsittelyn seuraaminen on helpompaa. Samalla väärinkäytösten mahdollisuus pienenee.

Kysymykseen 26. onko tietomurron varalle tehty suunnitelma ja määritelty vastuualueet, vastattiin 40% kyllä sekä 40% ei ja 20% ei osannut sanoa. Vastaukset ovat ristiriidassa mm. GDPR:n määräysten kanssa, sillä tietomurron sattuessa yrityksillä on 72 tuntia ottaa yhteyttä viranomaisiin olettaen, että murrossa on voitu päästä käsiksi henkilötietoihin. Hyvin suunniteltu strategia ja määrätyt vastuualueet nopeuttavat vahinkojen minimointia ja paluuta normaaliin.

6.3 Keskustelu

Tulosten analyysin jälkeen keskustellaan niiden merkityksestä vielä yleisemmällä tasolla. Tuloksien suppeus vaikeuttaa niiden analysoimista ja suurien johtopäätöksien vetämistä, mutta toisaalta myös niiden hajaantuneisuus vahvistaa käsitystä siitä, ettei käytänteet ole vakiintuneet alalla. Herättää myös huolta käytänteiden kehityksestä vastaukset kysymyksiin peruskivinä pidetyistä käytänteistä, jotka pätevät myös pilvipalveluiden ulkopuolella. Ottaen huomioon, että kysely oli kohdistettu tietoturvan ammattilaisille sekä sen, että kysymykset olivat pitkälti yksiselitteisiä, herää kysymys onko kyselyyn vastattu huolimattomasti?

Käytänteiden vakiinnuttaminen ei kuitenkaan välttämättä ole itseisarvo tietoturvallisuudessa yleisesti. Jokainen organisaatio on erilainen ja kohtaa erilaisia haasteita, joten tietoturvaa tulisi aina miettiä yrityksen oman ympäristön ja kontekstin kautta. Toisaalta tutkimus kohdistui julkisiin organisaatioihin, joiden konteksti on usein kohtalaisen samanlainen, vaikkakin pilvisiirtymät olivat eri vaiheissa.

Myös sopimuksiin liittyvissä kysymyksissä esiintyneet jakautuneet vastaukset ovat huolestuttavia julkisten organisaatioiden kannalta. Sopimusten tekeminen on yksi ainoista tavoista varmistaa asiakkaana hyvä asema palveluiden tason sekä tietoturvan kannalta. Sopimukset olisi hyvä räätälöidä aina omien tarpeiden mukaan, mutta isojen yritysten kanssa voi olla vaikea neuvotella ehdoista. Usein yritykset tarjoavat samanlaisia sopimuksia kaikille, jotta niiden käsittely on vaivatonta.

Hankinnan kannalta vastaukset olivat pitkälti odotettuja. Tulevaisuuden trendit oli huomioitu ja selkeä muutos kohti pilvipohjaisia palveluita on etenemässä. Keskeisiä kysymyksiä olivat myös palveluiden jatkuvuuteen liittyvät haasteet ja huolet. Vastaajat olivat kuitenkin ottaneet nämä huomioon hankintoja tehdessään ainakin osittain. Mielenkiintoa herätti myös riskien kartoittaminen, johon tutkimuksessa saatiin ristiriitaisia vastauksia. Riskejä oli siis kartoitettu, mutta ei välttämättä tarkkojen analyysien avulla vaan enemmän ajatuksen tasolla. Ulkopuolisia konsultteja tai vastaavia ei ollut käytetty, mutta niiden ammattitaidon hyödyntäminen voisi olla perusteltua. Markkinoiden tilannetta ja palveluntarjoajien tasoa voi olla vaikea hahmottaa ja seurata, minkä takia asiaan perehtyneet konsultit voisivat olla hyödyksi. Toisaalta heillä on kokemusta eri yritysten tilasta, joten konsultointi voisi avata uusia näkökulmia, vaikka varsinaista yhteistä projektia ei tulisikaan. Myös alan sertifikaatteihin paneutuminen sekä standardeihin tutustuminen vievät jo pitkälle palveluntarjoajan valitsemisessa tietoturvan kannalta.

Käytänteistä on tämän tutkimuksen avulla saatu alustava kuva, mutta vielä on paljon tutkittavaa ja erityisesti sopimusten asemaa tulisi myös jatkossa tutkia. Erityisesti EU:n Schrems II päätöksen jälkeen rekisterinpitäjille on tullut uudenlaista painetta varmistua tietoturvasta pilvipalveluissa. Tutkimuksen tuloksia ei voi yleistää, ja matalasta vastaus innosta johtuen herää kysymys oliko tutkimus liian aikaisin tehty. Pilvipalveluiden käyttöönotto oli kontaktoinnin yhteydessä käytyjen keskustelujen perusteella vielä monessa paikassa kesken.

7 YHTEENVETO

Tämän tutkielman tarkoituksena oli selvittää minkälaisia rajoitteita lait sekä säädökset asettavat pilvipalveluiden käytölle julkisella sektorilla sekä millaisia käytänteitä julkisilla organisaatioilla on pilvipalveluiden suhteen. Aihe oli rajattu julkiseen sektoriin, sillä tietoturvavaatimukset ovat hyvin erilaiset verrattuna yksityisten henkilöiden käyttämiin palveluihin. Tutkielman tutkimuskysymykset olivat seuraavanlaiset:

- *Mitä rajoitteita lait ja valtion linjaukset asettavat pilvipalveluiden käytölle?*
- *Millaisia käytänteitä julkisella sektorilla on pilvipalveluiden hankinnassa sekä käytössä*?

Tutkimus tehtiin kirjallisuuskatsauksena ja pohjautuu kandidaatintutkielmaan Pilvipalveluiden tietoturva – Yrityksen näkökulma. Kandidaatintutkielmasta on poimittu erityisesti pilvipalveluiden toimintaan liittyvää tietoa sekä mahdollisia uhkia. Tämän siksi että lukijan on hyvä ymmärtää pilvipalveluiden toimintaa sekä siihen kohdistuvia uhkia ennen rajoitteiden analysoimista. Pilvipalveluiden lakitekniset rajoitteet ovat hyvin samanlaiset kuin muillakin tiedonhallinnan alalla, mutta myös muutamia poikkeuksia löytyy. Näistä esimerkkinä pilvipalveluissa olevan tiedon nopea liikkuvuus sekä sijainti ja Suomen valtion pilvipalvelulinjaukset.

Pilvipalveluiden hyötyjä sekä yleistä toimintamallia kuvattiin tutkimuksessa, jotta lukijalle kasvaisi perusymmärrys siitä, miten pilvipalvelut toimivat sekä miksi ne ovat houkutteleva vaihtoehto yrityksille. Keskeisimpiä havaintoja pilvipalveluiden hyödyistä yrityksille olivat helppokäyttöisyys sekä kustannustehokkuus. Pilven tekninen toiminta jäi tarkoituksella pintapuoliseksi, sillä se ei ollut tutkimuksen kohde. Kuitenkin on hyvä huomata, että tarkempi tekninen ymmärrys saattaisi helpottaa tulosten analysoimista.

Pilvipalveluihin kohdistuvien uhkien määrittely oli hankalaa, johtuen niiden valtavasta määrästä. Esitellyt uhkat kuitenkin toistuivat useimmiten eri lähdekirjallisuudessa, joten ne valikoituivat tutkimuksen kohteiksi.

Keskeisimpänä uhkana pilvipalveluihin siirtymiselle yrityksen näkökulmasta oli luotettavuuden puute sekä skaalautumisen vaikeus. Luottamuksen puute liittyi palveluiden toiminnallisuuteen sekä tiedonkäsittelyn oikeellisuuteen. Toisaalta suuremmat yritykset eivät voi hyödyntää pilvipalveluita täysin, sillä valtava datan määrä on liikaa tämänhetkisillä resursseilla pilvipalveluille. Tutkimuksessa esitetyt uhkat ovat tämänhetkinen näkemys lähdekirjallisuuteen pohjautuen yleisimmistä ongelmista pilvipalveluissa. On kuitenkin tärkeä ymmärtää, että kaikkia uhkia ei ole välttämättä vielä löydetty tai ymmärretty tutkia.

Tietoturvaratkaisuja pilvipalveluihin kohdistuviin uhkiin oli myös erittäin paljon. Keskeisimmät ratkaisut pohjautuivat palveluntarjoajan sekä asiakasyritysten välisen toiminnan sääntelyyn lakien, sopimusten sekä tarkastusten avulla. Toisaalta myös teknisiä ratkaisuja oli lähdekirjallisuudessa paljon, mutta niiden osuus ei ollut niin merkittävä kuin luottamuksen kehittämisen. Nämä ratkaisut ovat päteviä tällä hetkellä, mutta pilvipalvelut sekä lait kehittyvät jatkuvasti ja samalla kehitetään uusia uhkia, jotka tekevät vanhoista tietoturvaratkaisuista toimimattomia.

Tutkimuksen tulosten perusteella voidaan todeta, että pilvipalveluiden tietoturva on kehittynyt ja jatkaa kehittymistä nopealla tahdilla. Tutkimuksen perusteella pilvipalveluiden tietoturvaan vaikuttavat palveluntarjoajan sekä asiakasyrityksen omat toimet valtavasti. Asiakkaan suorittaessa tarkan taustatutkimuksen palveluntarjoajasta sekä ohjeistamalla omat työntekijät hyviin käytänteisiin, pilvipalveluita on kohtuullisen turvallista käyttää. Myös kansainvälisesti on aloitettu tietoturvan kehittäminen, ja lainsäädännön muutokset tukevat pilvipalveluiden tietoturvallisuutta. Onkin tärkeä huomioida, että valtiovarainministeriö suosittelee käyttämään pilvipalveluita, mikäli ne tarjoavat parhaan hyödyn eikä muita esteitä ole. Uhkat ja palveluiden hyödyllisyys ovat kuitenkin pitkälti tapauskohtaisia, joten ei voida antaa kaikenkattavaa vastausta siihen voiko kaikkiin pilvipalveluihin luottaa.

Pilvipalvelut ovat nykyisin arkipäivää ja on paljon yrityksiä, jotka hyödyntävät niitä ainakin osittain päivittäisessä toiminnassaan. Pilveen liittyy kuitenkin ongelmia tiedon turvallisen käsittelyn kannalta, ottaen huomioon GDPR:n tiukat vaatimukset. Toisaalta useat pilvipalveluiden tarjoajat ovat peräisin Yhdysvalloista, jonka kanssa EU vuonna 2020 perui yhteistyösopimuksen tiedon turvallisen liikkumisen kannalta, mikä siirsi vastuun rekisterinpitäjälle. Toisin sanoen rekisterinpitäjän tulisi pystyä varmistumaan palveluntarjoajan luotettavuudesta tiedonkäsittelyn saralta. Voi kuitenkin olla vaikea neuvotella yksilöityjä sopimuksia mitkä estäisivät mm. lainvalvojia tutkimasta tietoa Yhdysvalloissa.

Tulevaisuuden tutkimuksen tulisi keskittyä erityisesti EU:n Schrems II päätöksen tulevaisuuden vaikutuksiin. Tällä hetkellä on vaikea ottaa kantaa mitkä sen vaikutukset ovat ja miten mahdollinen uusi sopimus tulee muuttamaan käytänteitä sekä pilvipalveluiden rajoitteita. Toisaalta julkisten organisaatioiden käytänteitä tulisi myös tutkia lisää, sillä tämän tutkimuksen tulokset eivät ole yleistettävissä hyviksi käytänteiksi, vaan tutkimuksen

tarkoitus on luoda katsaus tämänhetkiseen tilanteeseen. Tämä tutkimus ei kuitenkaan ota kantaa käytänteiden laatuun, mikä on myös haastava aihe, sillä alalla ei ole yhteneviä käytänteitä.

Tämän tutkimuksen rajoitteena on empiirisen osuuden heikko vastausinto, mikä tuli myös tutkijalle yllätyksenä. Ensimmäisten kontaktointien perusteella sekä tutkimuksen alussa saatu positiivinen kannustus aiheen pariin ei antanut syytä odottaa heikkoa kiinnostusta.

LÄHTEET

Accorsi, R., Lowis, L., & Sato, Y. (2011). Automated certification for compliant cloud-based business processes. *Business & Information Systems Engineering*, *3*(3), 145.

Anthes, G. (2010). Security in the cloud. *Communications of the ACM*, 53(11), 16-18.

Ardagna, C. A., Asal, R., Damiani, E., & Vu, Q. H. (2015). From security to assurance in the cloud: A survey. *ACM Computing Surveys (CSUR)*, 48(1), 12-30.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Gunho, L., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, *29*(3), 157-188.

Euroopan Unioni. (2020) Euroopan tietosuojaneuvosto otti kantaa Schrems II -päätökseen ja käsitteli PSD2-maksupalveludirektiiviä koskevaa ohjetta. Haettu 30.3.2021 osoitteesta: https://tietosuoja.fi/-/euroopan-tietosuojaneuvosto-otti-kantaa-schrems-ii-paatokseen-ja-kasitteli-psd2-maksupalveludirektiivia-koskevaa-ohjetta

Euroopan Unioni. (2012) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Unleashing the Potential of Cloud Computing in Europe.

Euroopan Unioni. (2016a). EU-US Privacy Shield. Haettu 3.4.2018 osoitteesta: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

Euroopan Unioni. (2016b). Adequacy of the protection of personal data in non-EU countries. Haettu 3.4.2018 osoitteesta: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

Erickson, M. L., & Gibbs, J. P. (1975). Specific versus general properties of legal punishments and deterrence. *Social Science Quarterly*, 390-397

Garrison, G., Kim, S., & Wakefield, R. L. (2012). Success factors for deploying cloud computing. *Communications of the ACM*, *55*(9), 62-68.

Georgiopoulou, Z., Makri, E. L., & Lambrinoudakis, C. (2020). GDPR compliance: proposed technical and organizational measures for cloud provider. *Information & Computer Security*.

Gupta, D., Lee, S., Vrable, M., Savage, S., Snoeren, A. C., Varghese, G., Voelkerg G. M. & Vahdat, A. (2010). Difference engine: Harnessing memory redundancy in virtual machines. *Communications of the ACM*, 53(10), 85-93.

Henry, S., & ALI, M. L. (2017). Cloud Computing Security Threats and Solutions. *i-manager's Journal on Cloud Computing*, *4*(2), 1

Hon, W. K., Hörnle, J., & Millard, C. (2012). Data protection jurisdiction and cloud computing–when are cloud users and providers subject to EU data protection law? The cloud of unknowing. *International Review of Law, Computers & Technology*, 26(2-3), 129-164.

IBM. (2020) Cost of a data breach. Haettu 22.5.2021: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Jaatun, M. G., Pearson, S., Gittler, F., Leenes, R., & Niezen, M. (2016). Enhancing accountability in the cloud. *International Journal of Information Management*. 1-11.

Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. *Current Journal of Applied Science and Technology*, 396-403.

Kissel, R. (Ed.). (2011). *Glossary of key information security terms*. Diane Publishing. 94

Kumar, N. S., Lakshmi, G. R., & Balamurugan, B. (2015). Enhanced attribute based encryption for cloud computing. *Procedia Computer Science*, 46, 689-696.

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science*, *125*, 691-697.

Kyberturvallisuuskeskus. (2020) Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). *Traficomin julkaisuja 13/2020*

Lango, J. (2014). Toward software-defined slas. *Communications of the ACM*, 57(1), 54-60.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53.

Narayanan, V. (2011). Harnessing the cloud: international law implications of cloud-computing. *Chi. J. Int'l L.*, 12, 783-809.

Neumann, P. G. (2014). Risks and myths of cloud computing and cloud storage. *Communications of the ACM*, *57*(10), 25-27.

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, *88*, 101608.

Ramachandran, M., & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management*, 36(4), 618-625.

Rani, B. K., Rani, B. P., & Babu, A. V. (2015). Cloud Computing and Inter-Clouds–Types, Topologies and Research Issues. *Procedia Computer Science*, *50*, 24-29.

Snook, C., & Harrison, R. (2001). Practitioners' views on the use of formal methods: an industrial survey by structured interview. *Information and Software Technology*, *43*(4), 275-283.

Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software*, 86(9), 2263-2268.

Ryan, M. D. (2011). Cloud computing privacy concerns on our doorstep. *Communications of the ACM*, *54*(1), 36-38.

Shahzad, F. (2014). State-of-the-art survey on cloud computing security Challenges, approaches and solutions. *Procedia Computer Science*, 37, 357-362.

Singh, S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75, 200-222.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & management*, *46*(5), 267-270.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97-100.

Srivastava, H., & Kumar, S. A. (2015). Control framework for secure cloud computing. *Journal of Information Security*, *6*(1), 12.

Sunyaev, A., & Schneider, S. (2013). Cloud services certification. *Communications of the ACM*, 56(2), 33-36.

Tian, L. Q., Lin, C., & Ni, Y. (2010). Evaluation of user behavior trust in cloud computing. International Conference on Computer Application and System Modeling (ICCASM) (Vol. 7, 7-567). *IEEE*.

Tietosuojavaltuutetun toimisto, (2020). Haettu 19.11.2020. (www.tietosuoja.fi/gdpr).

Valtiovarainministeriö. (2018). Julkisen hallinnon pilvipalvelulinjaukset. Valtiovarainministeriön julkaisu – 35/2018.

Viestintäviraston Kyberturvallisuuskeskus. (2014). Pilvipalveluiden tietoturva organisaatioille. Haettu 3.2.2018 osoitteesta: https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Yan, Q., & Yu, F. R. (2015). Distributed denial of service attacks in software-defined networking with cloud computing. *IEEE Communications Magazine*, 53(4), 52-59.

Zaharia-Rădulescu, A. M., & Radu, I. (2017). Cloud computing and public administration: approaches in several European countries. In *Proceedings of the International Conference on Business Excellence* (Vol. 11, No. 1, pp. 739-749). Sciendo.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83-93.