Teemu Reponen

# PILVIPALVELUIDEN TIETOTURVA – YRITYKSEN NÄKÖKULMA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

# TIIVISTELMÄ

Reponen, Teemu
Pilvipalveluiden tietoturva – Yrityksen näkökulma
Jyväskylä: Jyväskylän yliopisto, 2018, 24 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Pirhonen, Maritta

Tässä tutkielmassa tutkitaan pilvipalveluiden tietoturvallisuutta yritysten näkökulmasta. Erityisesti tarkastelussa on se kuinka tietoturvaa sekä luottamusta voidaan parantaa. Tässä kontekstissa tietoturvalla viitataan pilvipalvelussa olevan tiedon eheyteen sekä ulkoisten uhkien torjumiseen. Toisaalta luottamus viittaa pilvipalveluiden toimintojen sekä tietojenkäsittelyn luotettavuuteen. Tutkimus suoritettiin kirjallisuuskatsauksena ja keskeisimpinä löytöinä olivat kuvaus yleisimmistä tietoturvauhkista, joita pilvipalveluissa kohdataan. Lisäksi tutkimuksen tuloksena on konkreettisia metodeja pilvipalveluiden tietoturvan toteutukseen. Tulosten ohella tutkimus antaa pohjan tulevaisuuden tutkimukselle, jonka tulisi kohdistua pilvipalveluiden tiedon prosessointiin liittyvien ongelmien ratkaisuun.

Asiasanat: pilvipalvelu, tietoturva, luotettavuus, tietoturvauhkat

# ABSTRACT

Reponen, Teemu
Information security in Cloud services – A Business view
Jyväskylä: University of Jyväskylä, 2018, 24 s.
Information systems science, Bachelor thesis
Supervisor: Pirhonen Maritta

This thesis aims to investigate the state of information security in cloud based services, that are intended for corporate usage. The focus of this thesis is mainly on how to improve the accountability and information security of said services. In this context information security is defined as maintaining the integrity of the information stored in a cloud environment as well as protecting the cloud from external threats. On the other hand, accountability is defined as ensuring the functionality of the cloud and proper handling of data from the service provider. This thesis was conducted as a literature review and as a result the reader should have an overview of the most common threats faced in a cloud environment as well as an understanding of the basic functions of a cloud service. Furthermore, methods to improve information security in a cloud service can be found in the results. In addition, to the other results, this thesis provides a solid basis for further investigation on the dilemma of processing power within the cloud.

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

# KUVIOT

# 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.

Tämä tutkimus vastaa kirjallisuuskatsauksen avulla seuraaviin tutkimuskysymyksiin:

- Miten pilvipalveluiden tietoturvaa kehitetään?
- Kuinka pilvipalveluiden luotettavuutta voidaan parantaa?

Tavoitteena on löytää lähdekirjallisuudesta konkreettisia esimerkkejä siitä millä metodeilla pilvipalveluiden tietoturva on toteutettu ja kuinka sitä kehitetään eteenpäin. Toisaalta tutkimus selvittää miten pilvipalveluiden luotettavuutta voidaan kehittää eri keinoin. Lähdekirjallisuudesta löytyvät valtavat määrät tietoturvauhkia sekä pilvipalveluiden alati jatkuva kehitys luovat tarpeen tälle

tutkimukselle. Aihetta on tutkittu paljon, mutta pilvipalveluiden toiminta sekä käyttötarkoitus muuttuu 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”, ”Security solutions” 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 oltu 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.

Tutkimuksen tuloksena oli yleinen kuva suurimmista tietoturvauhkista, joita pilvipalveluihin kohdistuu sekä ratkaisuista jotka vastaavat ko. uhkiin. Tutkimuksessa selvisi selvä kahtiajako pilvipalveluiden tietoturvan määrittelyssä. Yhtäältä tietoa suojataan teknisillä ratkaisuilla, kuten salaamalla tieto tai seuraamalla pilvipalveluiden käyttöä. Toisaalta tietoturvaa parannetaan lainsäädännöllä, hyvillä käytänteillä sekä sopimuksilla. Toinen on siis selvästi tekninen ratkaisu ja vastaa teknisiin ongelmiin, kun taas toinen lähestymistapa haluaa kasvattaa luottamusta ja läpinäkyvyyttä pilvipalveluiden toimintaa kohtaan. Tutkimuksen tulokset eivät kuitenkaan pysty antamaan yksiselitteistä vastausta siihen onko yrityksen turvallista ladata tietoja pilveen. Tulokset kuitenkin antavat konkreettisia keinoja tietoturvallisuuden kehittämiseen sekä luotettavuuden parantamiseen. Samalla tutkimus luo pohjan tulevaisuuden tutkimukselle tuomalla esiin pilvipalveluiden ongelmia, joita ei vielä ole ratkaistu ja jotka vaikeuttavat tietoturvan kehittymistä.

Tutkimus on jaettu kolmeen sisältölukuun, joista ensimmäinen on Pilvipalvelut. Ensimmäisessä sisältöluku luo teoreettista taustaa pilvipalveluiden toiminnasta ja toimijoista. Ilman toiminnan sekä 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. Lisäksi luvussa käsitellään pilvipalveluiden luotettavuuden määrittelyä lainsäädännön sekä sopimusten näkökulmasta. Toisaalta myös käyttäjien vastuuta tutkitaan, eli sitä kuinka asiakasyrityksen johto

sekä työntekijät pystyvät osaltaan vaikuttamaan pilvipalveluiden tietoturvallisuuteen.

Viimeisessä sisältöluvussa on lueteltu ratkaisuja aiemmissa luvuissa esitettyihin ongelmiin sekä käydään läpi miten tietoturvaa kehitetään. Tietoturvaratkaisuina on käsitelty mm. lainsäädäntöä, tiedon salausta sekä turvallisuussertifikaatteja. Lisäksi luvussa tuodaan esille ongelmia jotka vaikeuttavat pilvipalveluiden kehittymistä.

# 2 PILVIPALVELUT

Tässä luvussa esitellään pilvipalveluiden toimintaa, sekä sitä miksi näiden palveluiden käyttö on yrityksille kannattavaa.

## 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 puhelimille 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 1 Pilvipalvelumalli (Ravi Kumar ym., 2018, s. 692)

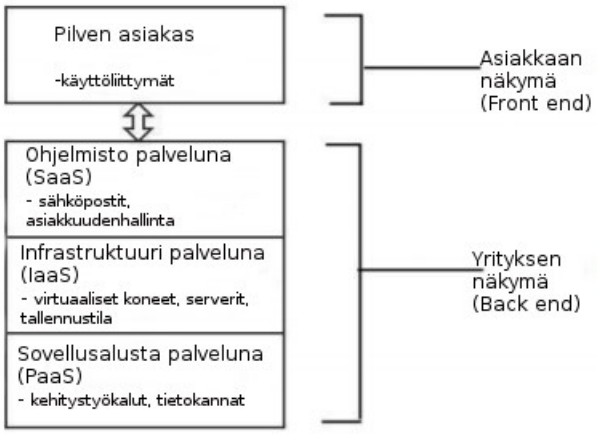
Pilvipalveluiden toimintamallissa asiakas maksaa palvelusta, jonka palveluntarjoaja toimittaa. Palveluntarjoajan ja asiakkaan välissä toimii palvelun välittäjä, joka välittää eli myy tuotteen asiakkaalle. Palveluntarjoajan alaisuudessa toimii palvelun toimittaja, joka vastaa pilven toiminnallisuudesta. Viimeiseksi, palve-

lun 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 2 Pilvipalveluiden rakenne (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 tietoteknis-

tä 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 ylläpito kustannuksia. (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 testaamisen, sillä virtuaaliympäristössä pystytään eristämään mahdolliset syntyvät ongelmat eivätkä ne vaikuta muihin tietokoneen toimintoihin. (Gupta ym., 2010)

# 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) 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 asiakas yrityksen 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 tie-

donkäsittely 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 sekä todennus prosessien 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.

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 toimintamallin 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 tarkoitus 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 tietoturva uhkista ja vaikeasti hallittavista osista on käyttäjä. (Öğütçü, Testik, & Chouseinoglou, 2016) 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.

Käyttäjällä on myös vastuu tiedosta, sillä pilvipalveluiden toiminta on vielä kehitysvaiheessa, eikä palveluiden toimintaan voi luottaa sokeasti. Tästä joh-

tuen 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 TIETOTURVARATKAISUT

Tässä luvussa käsitellään tietoturvaratkaisuja uhkiin, joita pilvipalveluihin kohdistuu. Uhkia on monenlaisia, eikä kaikkia välttämättä vielä edes tunneta, mutta tässä luvussa esitetyt ratkaisut vastaavat tunnetuimpiin sekä yleisimpiin uhkiin konkreettisten esimerkkien avulla.

## 4.1 Sopimukset ja lainsäädäntö

Pilvipalveluiden toimintaa on pyritty valvomaan useiden eri tahojen toimesta asettamalla lakeja, jotka luovat rajoitteita pilvipalveluiden tiedon käytön 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 siirtyy 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 käytää 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 tietosuoja käytänteitä eri maiden välillä. Tiedon suojelu toteutetaan määräämällä tiedon käsittelylle 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 tietosuoja käytänteitä sekä määrää vuosittaisen tarkastustapaamisen jossa varmistetaan käytänteiden toteutuksen. Tämän lisäksi EU on määritellyt perusteet riittävälle tiedonsuojaamiselle ja niiden perusteella listannu 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)

## 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.

Sertifiointi prosessi 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 liiketoiminta käytännöt kuten laadunhallinta ja taloudelliset realiteetit tulisi tarkastaa. 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, sekä vaikeuttaa markkinoiden toimintaa. Johtuen sertifiointi-prosessin 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 Tiedon salaus

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 homorfisella salauksen avulla pystytään tekemään sähköpostin roskapostifiltteri, 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)

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 ylläpi-

dossa. 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.

## 4.4 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 sekä Microsoft. Hewlett-Packard on suunnitellut Solu Palveluna prototyyppiä, joka automatisoisi pilvipalveluiden tietoturvan. Solut olisivat yhteydessä useisiin virtuaalisiinkoneisiin 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. Proto-

tyyppi 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 koneet sijaitsevat heille omistetuilla koneilla. Tämä ei kuitenkaan käytännössä välttämättä ole mahdollista, sillä ylläpitokustannukset kasvaisivat kohtuuttomiksi. (Anthes, 2010)

## 4.5 Tiedon käyttö ja saatavuus

Iso osa pilvipalveluiden tietoturvaa on tiedon käytön sekä pilveen 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, niin 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)

# 5 YHTEENVETO

Tämän tutkielman tarkoituksena oli selvittää yrityksille suunnattujen pilvipalveluiden tietoturvaa. Aihe oli rajattu yrityspalveluihin, sillä tietoturvavaatimukset ovat hyvin erilaiset verrattuna yksityisten henkilöiden käyttämiin palveluihin. Tutkielman tutkimuskysymykset olivat seuraavanlaiset :

- Miten pilvipalveluiden tietoturvaa kehitetään ?
- Kuinka pilvipalveluiden luotettavuutta voidaan parantaa ?

Tutkimus tehtiin kirjallisuuskatsauksena ja tietoturvauhkia niin kuin ratkaisujakin löytyi valtavasti. Tutkielmassa esitetyt uhkat sekä ratkaisut on valittu niiden yleisyyden perusteella tutkimusmateriaaleista, mutta ne eivät vältämättä anna koko kuvaa pilvipalveluiden tietoturvan tilasta.

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.

Pilvipalveuihin 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 tämän hetkisillä 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. Tietoturvaratkaisut voidaankin jakaa kirjallisuuden perusteella kahteen eri kategoriaan : luottamusta kehittävät ja turvallisuutta kehittävät ratkaisut. Ensimmäinen viittaa siis asiakkaiden ja palveluntarjoajan suhteiden kehittämiseen, kun taas jälkimmäinen on tiedon todellista turvaamista. Nämä ratkaisut ovat päteviä tällä hetkellä, mutta pilvipalvelut 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. 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 rajoituksia prosessointikapasiteetin ja sen myötä skaalattavuuden suhteen. Tulevaisuuden tutkimuksen tulisikin kohdistua näiden ongelmien ratkaisuihin, jotta pilpalveluiden kehitys voisi jatkua. Rajoitukset prosessointikyvyssä vaikeuttavat myös pilven tietoturvallisuuden kehittämistä, sillä useat salausmetodit vaativat paljon laskentatehoa ollakseen turvallisia.

# LÄHTEET

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.

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

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

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.

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.

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

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.

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

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*.

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.

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.

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.

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.

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.

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