Jaakko Kosonen

TIETOTURVA PILVIPALVELUISSA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2015

TIIVISTELMÄ

Kosonen, Jaakko
Tietoturva pilvipalveluissa
Jyväskylä: Jyväskylän yliopisto, 2015, 27 s.
Tietojärjestelmätiede, Kandidaatin tutkielma
Ohjaaja(t): Seppänen, Ville

Pilvipalvelut ovat uusi konsepti, joka tarjoaa mahdollisuuden ulkoistaa sovellukset ja laskentainfrastruktuurin internetiin kolmannelle osapuolelle. Pilvipalveluiden avulla on mahdollista vähentää IT-järjestelmien ylläpitokuluja ja helpottaa järjestelmän ylläpitoa. Kuitenkin suurin epävarmuustekijä pilvipalveluissa on tietoturva. Tämä tutkielma käsittelee pilvipalveluita ja niiden tietoturvaa ja riskejä, joita käyttäjä voi kohdata. Tutkielman pääpaino on yleisesti kohdattavissa tietoturvauhkissa ja niiden ehkäisemisessä

Aluksi tutkielmassa käydään läpi pilvipalveluita yleisesti ja esitellään pilvipalveluiden palvelutyyppien hierarkia, sekä yleisimmät käyttöönottomallit. Tämän jälkeen tutkielmassa keskitytään erilaisiin tietoturvauhkiin pilvilaskennassa, sekä esitellään muutamia reaalimaailmassa toteutuneita tietoturvaongelmia. Tutkielman viimeinen osa käy läpi, miten tietoturvaa voidaan parantaa loppukäyttäjän kannalta.

Tutkielma on toteutettu kirjallisuuskatsauksena ja perustuu hyväksi todettuihin, tieteellisiin lähteisiin. Saatujen tulosten perusteella suurimmat ongelmat pilvipalveluissa liittyvät käyttäjän ja palveluntarjoajan väliseen luottamukseen, sekä tietoliikenteen turvallisuuteen. Tutkielmasta myös selviää, että poikkeavat vaatimukset pilvipalveluiden tietoturvaan johtuvat pilvipalveluiden poikkeavista ominaisuuksista. Tämän lisäksi havaittiin myös, että tietoturvaan liittyviä ongelmia voidaan minimoida kehitettyjen tietoturvamallien ja käytänteiden avulla.

Asiasanat: pilvipalvelu, tietoturva, kolmas osapuoli, luottamus, ominaisuus

ABSTRACT

Kosonen, Jaakko
Information security in cloud computing
Jyväskylä: University of Jyväskylä, 2015, 27 p.
Information Systems, Bachelor's Thesis
Supervisor(s): Seppänen, Ville

Cloud services are a new concept, which makes possible to outsource softwares and computing resources in internet to a third party. With cloud services it is possible to reduce IT-system's maintenance costs and make easier to upkeep system. However, information security is considered to be the greatest problem in cloud services. The focus of this thesis is in cloud services and their information security and risks, that users may confront. The main focus of this thesis is in general information security threats and their prevention.

First in this thesis I will consider cloud computing in general and I will introduce a common hierarchy of cloud computing service models. After this the thesis concentrates in different kinds of security threats in a cloud computing and also introduces a few real world cloud computing issues. The last part of this thesis focuses on how to prevent information security threats in cloud computing in general.

This thesis is the review of a literature, found from high quality scientific sources. The most notable security issues in cloud computing are related to trust and telecommunications between the user and service provider. Also divergent information security requirements are due to divergent features in cloud computing. It is possible to reduce risks by different kinds of security models and practices.

Keywords: cloud service, information security, third party, trust, characteristic

KUVIOT

Kuvio 1 Yleinen pilvipalveluiden kerroksittainen hierarkia(Pallis 2010) 10
Kuvio 2 Tietoturvakehys pilvipalveluympäristölle 21

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

KUVIOT 4

SISÄLLYS 5

1 JOHDANTO 6

2 PILVIPALVELUT YLEISESTI 8
2.1 Pilvipalveluiden käyttöönottomallit 9
2.2 Pilvipalvelumallit 10
2.3 Pilvipalveluiden ominaisuudet 11

3 PILVIPALVELUIDEN TIETOTURVAONGELMAT 13
3.1 Tietoturvavaatimukset pilvipalveluissa 13
3.2 Tyypilliset tietoturvaongelmat pilvipalveluissa 15
3.2.1 Yleinen tietoturva 15
3.2.2 Saatavuus 16
3.2.3 Kolmas osapuoli 16
3.3 Esimerkkejä käytännön tietoturvaongelmista 17

4 TIETOTURVARATKAISUT PILVIPALVELUISSA 18
4.1 Tietoturvamallit pilvipalveluissa 18
4.1.1 TCCP 18
4.1.2 SecureCloud 20
4.2 Ratkaisuja tietoturvaongelmiin 21

5 YHTEENVETO JA POHDINTA 24

LÄHTEET 26

1 Johdanto

Pilvilaskenta on melko uusi konsepti, jonka voidaan mieltää muuttaneen suurta osaa informaatioteknologian kentästä. Pilvipalveluiden yleistyminen on vaikuttanut merkittävästi organisaatioiden toimintatapoihin IT-ratkaisuja kehittäessä. Pilvilaskennalla tässä yhteydessä tarkoitetaan laskennan ulkoistamista verkon yli ns. pilveen. Pilvipalveluilla voidaan tarkoittaa esimerkiksi verkon yli palveluiden muodossa tarjottavia ohjelmia tai loppukäyttäjän tarpeille skaalautuvaa IT-infrastruktuuria, kuten laskentatehoa.

Pilvipalveluiden käyttöönotto on nostanut suosiotaan organisaatioissa sen tuomien hyötyjen vuoksi, myös viime vuosina aiheesta on tehty paljon kattavaa tieteellistä tutkimusta. Pilvipalveluiden suuri suosio perustuu niiden ominaisuuksiin, joita ovat mm. resurssien skaalautuvuus ja alhaiset kustannukset verrattuna perinteisiin toimintamalleihin. Tämä lisää pilvipalveluiden käyttöönoton houkuttelevuutta organisaation, yrityksen tai muun loppukäyttäjän näkökulmasta.

Etujen lisäksi pilvilaskenta on herättänyt huolia liittyen yksityisyyteen, tietoturvaan ja luotettavuuteen. Koska asiakkaan data lähetetään verkon yli palveluntarjoajalle säilytettäväksi datavarastoihin on yksityisyyden turvaaminen avainasemassa, koska data voi olla arkaluontoista. Myös omistussuhde dataan on herättänyt kysymyksiä pilvilaskennan kentällä. Kenen omistuksessa ja käytettävissä lopulta data on, koska se sijaitsee organisaation ulkopuolisen toimijan hallussa. Myös salakuuntelu ja arkaluontoisen tiedon urkkiminen herättää kysymyksiä pilvipalveluiden käyttöönotossa.(Hayes, 2008.)

Tutkielmani tarkoitus on antaa kattava kuva pilvipalveluista yleisesti, sekä esitellä keskeisimmät ominaisuudet. Tutkielmassa myös perehdytään pilvilaskentaan liittyviin tietoturvauhkiin. Tietoturvan tarkempi käsittely pyrkii antamaan kuvan, millaisia tietoturvariskejä voidaan kohdata pilvipalveluissa ja miten pilvipalveluiden turvallisuutta voidaan parantaa loppukäyttäjän näkökulmasta. Pilvipalveluita ja tietoturvaa lähestytään tutkimuksessa erityisesti asiakkaan, kuten organisaation tai yrityksen näkökulmasta.

Tutkimus toteutetaan kirjallisuuskatsauksena, joka pohjautuu tieteellisiin lähteisiin. Lähteiden haku keskittyy lähinnä informaatioteknologian alueella

toimiviin, luotettaviin tietokantoihin kuten IEEE Xploriin ja ACM Digital Libraryyn. Myös Jyväskylän Yliopiston JYX –tietokantaa ja Google Scholaria käytetään tutkimuksen lähdeaineiston etsimisessä.

Tutkimuskysymykset ovat: ”Millaisia ovat erilaiset pilvipalveluissa kohdattavat tietoturvariskit?” ja ”Miten pilvipalveluiden turvallisuutta voidaan parantaa loppukäyttäjän kannalta?” Motiivit tutkimukseen ovat oma mielenkiinto aihealuetta ympyröivään keskusteluun, pilvipalveluiden yleistyminen organisaatiotasolla. Tietoturva tutkimusaiheena on mielenkiintoinen, koska sitä pidetään yleisesti suurimpana riskinä pilvipalveluiden käytössä. Tutkimus myös tarjoaa kattavan pohjan empiiriselle jatkotutkimukselle.

Tutkimuksen tuloksena selviää millaisia riskejä esiintyy pilvipalveluissa sekä miten turvallisuutta voidaan parantaa pilvipalveluita käyttäessä. Tutkimuksen tulokset antavat tietoa siitä onko pilvipalveluiden tietoturvallisuuteen liittyvät uhat loppukäyttäjän kannalta merkittäviä ja miten esiintyviä uhkia voidaan ehkäistä turvallisuuden kannalta.

Tutkielman rakenne on seuraava. Toisessa luvussa käsitellään pilvipalvelut käsitettä yleisesti ja esitellään mistä pilvipalvelut muodostuvat. Kolmannen luvun aiheena on pilvipalveluiden tietoturvaongelmat. Aihetta käsitellään pilvipalveluiden yleisten tietoturvavaatimusten ja yleisimpien tietoturvaongelmien saralta. Tutkielman neljäs luku keskittyy pilvipalveluiden tietoturvaongelmien ratkaisuihin. Viides luku sisältää yhteenvedon ja pohdintaa tutkielmasta, sekä esittelee mahdolliset jatkotutkimuskysymykset.

2 Pilvipalvelut yleisesti

Tässä luvussa määritellään pilvipalvelu käsitteenä yleisellä tasolla. Luvussa käsitettä tarkastellaan käymällä ensiksi läpi eri käyttöönottomallit pilvipalveluissa, jonka jälkeen esitellään yleisesti tarjottavat eri pilvipalvelumallit. Viimeisenä luvussa käydään läpi pilvipalveluiden ominaisuudet.

Pilvipalveluille ei ole yhtä vakiintunutta määritelmää, vaan viimeisten kymmenen vuoden aikana erilaisia määritelmiä on esitetty useita. Pilvipalveluiden käsitetään yleensä tarkoittavan palveluita, joita tarjotaan Internetin yli käyttäjälle, sekä laitteistoa ja ohjelmistoja, joita operoidaan datakeskuksista käsin (Armbrust ym., 2010). Palveluita tällaisessa tapauksessa tarjoaa palveluntarjoaja ja kyseessä on julkinen pilvi eli palveluita voi ostaa lähes kuka vaan. Organisaatiot voivat myös operoida omaa palvelinkeskustaan omiin tarpeisiinsa ja tällöin kyseessä on yksityinen pilvi. Julkisen ja yksityisen pilven välimuotoa kutsutaan nimellä hybridipilvi. (Armbrust ym., 2010) Pilven käyttöönottomallit käydään tarkemmin läpi alaluvussa 2.1.

Pilvipalvelut käsitetään yleisesti koostuvan kolmesta eri kokonaisuudesta, jotka ovat hierarkisesti yhteydessä toisiinsa. Näitä kokonaisuuksia ovat infrastruktuuri palveluna(Infrastructure as a Service, IaaS), sovellualusta palveluna(Platform as a Service, Paas) ja ohjelmisto palveluna(Software as a Service, SaaS). (Miller & Veiga, 2009.) Näitä kutsutaan pilvipalvelumalleiksi ja ne otetaan myös tarkasteluun alaluvussa 2.2.

Pilvipalveluiden idea on siis varsin yksinkertainen. Palveluntarjoaja tarjoaa loppukäyttäjälle Internetin yli ohjelmistot, sovellualustat ja infrastruktuurin. Asiakkaan data tallennetaan palvelinkeskuksiin ja se on loppukäyttäjälle saatavilla ympärivuorokautisesti. Internetin yli tapahtuva tarjonta mahdollistaa teoriassa rajattomat resurssit asiakkaalle. Loppukäyttäjä ei tarvitse toimiakseen muuta kuin Internet-yhteyden ja päätelaitteen. Perinteiseen IT-malliin verrattuna, jossa ostetaan omaksi kaikki resurssit ja huolehditaan niiden ylläpidosta, pilvipalvelut ovat joustava ja edullinen vaihtoehto.

2.1 Pilvipalveluiden käyttöönottomallit

Kuten jo johdannossa todettiin, pilvipalveluiden idea on varsin yksinkertainen. Loppukäyttäjä ei välttämättä tiedä datakeskuksen varsinaista sijaintia, mutta laitteistot ja ohjelmistot operoivat kokonaan kolmannen osapuolen palvelimilla datakeskuksissa. Koska loppukäyttäjä ei tiedä palvelinten fyysistä sijaintia, voidaan tätä paikkaa kutsua esimerkiksi pilveksi.

Pilvipalvelut voidaan ottaa käyttöön eri tavoin, jolloin puhutaan pilvipalveluiden käyttöönottomalleista. Tieteellisissä julkaisuissa yleisimmät vastaan tulevat käyttöönottomallit ovat: julkinen pilvi, yksityinen pilvi ja hybridipilvi. Näihin eri malleihin ja niiden eroihin perehdytään tässä luvussa.

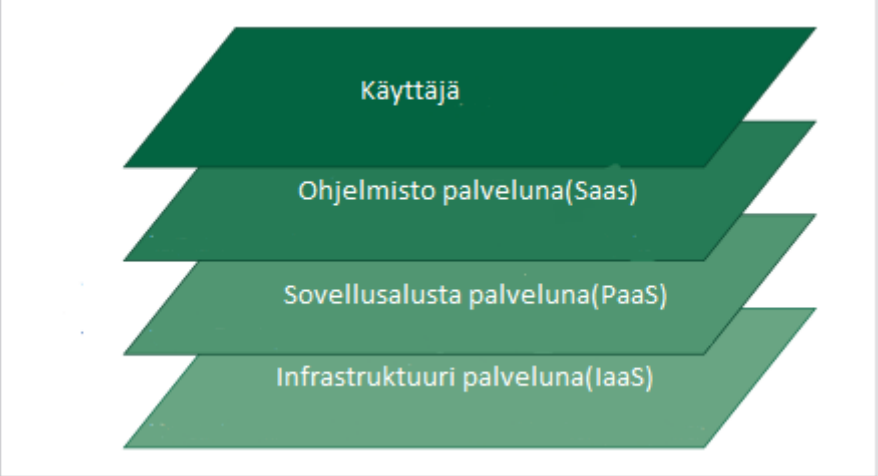
Julkinen pilven toimintaperiaate on, että infrastruktuuri ja ohjelmistot ovat kaikkien käyttäjien saatavilla Internetin yli. Infrastruktuuria ja ohjelmistoja operoidaan datakeskuksista käsin ja ne omistaa palveluntarjoaja. Julkisen pilven palvelut ovat kaikkien saatavilla eli yritykset voivat ostaa resursseja käyttöönsä tarpeen mukaan ja käytännössä milloin vain (Jansen & Grance, 2011). Hinnoittelu toimii ”pay-as-you-go” –mallin mukaisesti eli loppukäyttäjä maksaa vain ja ainoastaan niistä resursseista, joita käyttää (Armbrust ym., 2011). Julkisen pilven palvelut ovat oivallisia pienille tai aloittaville yrityksille ja tavallisille kuluttajille.

Yksityinen pilvi on taas malli, jossa pilven resursseja ja palveluita operoi yksittäinen organisaatio tai yritys. Palveluiden hallinnasta vastaa organisaatio itse, mutta myös erillinen kolmas osapuoli voi ottaa vastuun. Suurin ero julkisen ja yksityisen pilven välillä on, että yksityisessä pilvessä resursseja ei vuokrata vaan ne omistaa organisaatio itse. Yksityisen pilven mallissa organisaation data säilötään organisaation omassa datakeskuksessa. (Jansen & Grance, 2011.) Yksityinen pilvi mahdollistaa suuremman kontrollin infrastruktuurin ja resurssejen hallinnoimiseen kuin julkinen pilvi. Yksityisen pilven tapauksessa organisaation toiminta pitää olla tarpeeksi suurta, jotta hyödyt pilven käyttöönotosta ovat suuremmat kuin kustannukset. (Armbrust ym., 2011.)

Kahden edellä mainitun käyttöönottomallin välimuotoa kutsutaan hybridipilveksi. Hybridipilven avulla voidaan saavuttaa sekä julkisen, että yksityisen pilven edut. Hybridipilven avulla voidaan saavuttaa alhaiset kustannukset ja palveluiden tehokas käyttö. (Li, Wang, Li, Li, Wang & Du, 2013.) Hybridipilven avulla loppukäyttäjä pystyy hallinnoimaan resurssejaan paremmin, mutta julkisen pilven ominaisuuksien myötä myös loppukäyttäjällä on laajemmat palvelut käytettävissään.

2.2 Pilvipalvelumallit

Mellin ja Grancen (2011) mukaan pilvipalvelumallit koostuvat kolmesta tasosta: infrastruktuuri palveluna, sovellusalusta palveluna ja ohjelmisto palveluna. Monesti pilvipalveluiden ajatellaan tarkoittavan vain ohjelmiston tarjoamista palveluna, mutta pilvipalveluina ohjelmistojen lisäksi tarjotaan myös laitteistoresursseja ja sovellualustoja palveluna.



Kuvio 1 Yleinen pilvipalveluiden kerroksittainen hierarkia(Pallis 2010)

Infrastruktuuri palveluna eli IaaS–malli tarjoaa käyttäjälle infrastruktuuriresursseja tarpeen mukaan. Resursseja joita voidaan tarjota ovat esimerkiksi laskentakapasiteetti, tallennustila ja tietoliikenneyhteydet. Käyttäjä ei voi hallita ja kontrolloida taustalla pyörivää pilvi-infrastruktuuria, mutta voi kontrolloida käyttöjärjestelmää, tallennustilaa ja asennettuja ohjelmistoja. Myös tiettyjen tietoliikenneyhteyksiin liittyvien ohjelmistojen osien, esimerkiksi palomuuri, rajoitettu kontrollointi on mahdollista loppukäyttäjälle.(Mell & Grance, 2011.)

Sovellusalusta palveluna eli PaaS-malli tarjoaa käyttäjälle alustan ja työkalut sovellusten kehittämiseen, hallinointiin ja säilyttämiseen. Kuluttaja ei voi kuitenkaan käyttää tai hallinnoida taustalla pyörivää infrastuktuuria (Mell & Grance, 2011). Käyttäjä ei siis hallinnoi laitteistoresursseja vaan ostaa sovellusalustan palveluna käyttöönsä. PaaS-mallissa käyttäjä voi kehittää sovelluksia palveluntarjoajan palvelimilla, jolloin hänen ei itse tarvitse ostaa ja huolehtia sovelluskehitystyökaluista, eikä niiden pyörittämiseen tarvittavasta infrastruktuurista.

Ohjelmisto palveluna eli Saas-malli on viimeinen ja tutkimuksen kannalta myös tärkein osa pilvipalveluiden hierarkiaa. Saas- eli Software as a Service –mallissa käyttäjät ostavat käyttöoikeudet ohjelmistoille, mutta tieto tallentuu palveluntarjoajan palvelimelle. Ohjelmisto palveluna mallissa ohjelmistot ovat käyttäjän käytettävissä tarpeen mukaan Internet –yhteyden yli. Ohjelmistoja voidaan käyttää kevyillä käyttöliittymillä, esimerkiksi Internet-selaimella, tai

perinteisemmin ohjelmiston omalla käyttöliittymällä (Mell & Grance, 2011). Internet-selaimella tarjottaviin ohjelmistojen pyörittämiseen ei loppukäyttäjä tarvitse kuin päätelaitteen ja selaimen. SaaS-mallissa yksinkertaisesti käyttäjän ohjelmat ovat käynnissä palveluntarjoajan palvelimilla. Täten SaaS-palveluntarjoaja ottaa vastuun palvelimista ja ohjelmistoista sekä näihin liittyvästä toiminnasta. Ohjelmistojen toimintaan sisältyy esimerkiksi asennus, päivittäminen ja varmuuskopiointi. Ohjelmiston käyttäjä saa haltuunsa ohjelman ja tarpeelliset hallintaoikeudet. (Waters, 2005.)

2.3 Pilvipalveluiden ominaisuudet

Pilvipalveluihin liittyvíssä tutkimuksissa ja NIST:in (National Institute of Standards and Technology) määritelmässä tunnistetaan viisi kohtaa, joiden ajatellaan olevan yleisimmät yhdistävät ominaisuudet pilvipalveluissa. Nämä viisi ominaisuutta ovat: itsepalvelu, laaja käytettävyys verkon kautta, resurssien yhdistäminen, nopea joustavuus ja mitattava palvelu. NIST:in määritelmä on laadittu teknisestä näkökulmasta, mutta mielestäni määritelmä kuvaa hyvin pilvipalveluiden yleisiä ominaisuuksia.

Itsepalvelulla tarkoitetaan, että käyttäjä voi ottaa automaattisesti käyttöönsä tietoteknisiä resursseja, kuten suoritustehoa, tallennustilaa tai erilaisia ohjelmistoja. Käyttäjän ei tarvitse näitä resursseja saadakseen olla kontaktissa esimerkiksi asiakaspalvelijan kanssa, vaan hän voi ostaa ne käyttöönsä palveluntarjoajalta ilman välikäsiä. (Mell & Grance, 2011.)

Laaja käytettävyys verkon kautta tarkoittaa, että pilvipalveluiden kaikki ominaisuudet ovat käytettävissä asiakkaalle verkon, esimerkiksi Internetin, kautta. Pilvipalvelut ovat käytettävissä myös milloin vain ja niitä pääsee käyttämään eri alustojen kautta(esim. kannettava tietokone, tabletti, älypuhelin ja työpääte). Näitä resursseja on mahdollista käyttää asiakassovelluksilla, jotka sijaitsevat asiakkaan omilla sivuilla.(Dillon, Wu, & Chang, 2010; Mell & Grance, 2011.)

Resurssien yhdistäminen tarkoittaa, että palveluntarjoajan tarjoamat tietotekniset resurssit ovat yhdistetty. Tällä tavalla pyritään palvelemaan useita asiakkaita, joko virtualisointimallia tai monivuokrasuhdetta käyttämällä. Näissä erilaiset fyysiset ja virtuaaliset resurssit on määritelty kysynnän mukaan. Tälläistä mallia kutsutaan ”pool-pohjaiseksi” malliksi. Tälläisellä mallilla voidaan saavuttaa suuresta mittakaavasta johtuen taloudellista säästöä ja myös erikoistua paremmin pienempiin kokonaisuuksiin. Myös fyysinen laskentateho on asiakkaalle näkymätöntä, joten ei voida tietää missä fyysisessä paikassa tai muodossa asiakkaan resurssit ovat. (Dillon ym., 2010; Heino, 2010; Mell & Grance, 2011.)

Nopealla joustavuudella tarkoitetaan, että asiakkaan tietotekniset resurssit eivät ole niinkään pysyviä, vaan nopeita ja muotoutuvia. Asiakas voi nostaa ja vähentää resursseja milloin vain, sen hetkisen tarpeen mukaan. Mikään etukäteissopimus tai sitoumus ei estä tätä. Resurssien laskeminen tai

nostaminen riippuu myös sopimustyypistä, joidenkin sopimusten kohdalla tietoteknisten resurssien laskeminen ei ole mahdollista. Asiakkaan näkökulmasta resurssit ovat äärettömiä ja kapasiteettiä voidaan nostaa milloin vain vastatakseen sen hetkiseen kulutuspiikkiin tehokkaammin. (Dillon ym., 2010; Mell & Grance, 2011.)

Mitattavalla palvelulla pilvipalveluiden yhteydessä tarkoitetaan, että vaikka tietotekniset resurssit ovat käyttäjille yhteisiä ja jaettuja, pystytään silti mittaamaan tietyin menetelmin yksittäisen asiakkaan resurssien käyttö (Dillon ym., 2010). Tämä tarjoaa käyttäjälle avoimuutta, jolloin asiakas maksaa vain käyttämistään resursseista. Resurssien käyttöä voidaan monitoroida, kontrolloida ja raportoida, jolloin ulkoistetun palvelun käytön läpinäkyvyys varmistetaan sekä käyttäjälle, että myös palveluntarjoajalle. (Heino, 2010; Mell & Grance, 2011.)

3 Pilvipalveluiden tietoturvaongelmat

Tietoturvaa pidetään pilvipalveluissa yhtenä merkittävimpänä ongelmana ja sen ympärillä on tehty paljon tutkimusta viime vuosina. Yksi suurimmista huolenaiheista pilveen siirryttäessä on juuri tietoturva. Asiakkaan näkökulmasta epävarmuutta aiheuttaa, että palveluntarjoajalla on täysin rajaton pääsy asiakkaan dataan. Myös huolta aiheuttaa seikka, että pilvessä toimiva verkkopalvelu on korkeintaan yhtä luotettava kuin pilvipalvelukin. Myös perinteisemmät tietoturvaongelmat ovat läsnä pilvipalveluissa, joka osaltaan lisää riskiä käyttäjän näkökulmasta.

Tässä luvussa käydään ensiksi läpi yleiset tietoturvavaatimukset pilvipalveluissa. Tämän jälkeen tutkimuksessa käydään läpi yleisimmät tunnistetut tietoturvaongelmat ja viimeisessä alaluvussa käsitellään esimerkkejä reaalimaailmassa toteutuneista tietoturvaongelmista pilvipalveluissa.

3.1 Tietoturvavaatimukset pilvipalveluissa

Tässsä alaluvussa käydään läpi vaatimukset, jotka edellytetään saavutettaviksi tietoturvalliselta palvelulta yleisellä tasolla. Monet läpikäytävistä vaatimuksista koskevat erityisesti IaaS-palveluntarjoajaa ja IaaS-asiakasta, mutta vaatimukset sivuuttavat myös koko pilvipalvelukonseptia. Tyypillinen tapaus pilvipalveluissa on, että asiakas siirtää fyysisen laitteiston ylläpidon palveluntarjoajalle. Asiakkaan näkökulmasta tämän ajatellaan monesti olevan yksi suurimmista eduista pilvipalveluihin siirryttäessä. Eduista huolimatta on se myös yksi suurimmista huolenaiheista pilvipalveluissa. Siirrettäessä esimerkiksi laitteiston ylläpidon palveluntarjoajalle, menettää asiakas samalla laitteiston fyysisen hallinnan, joutuu jakamaan fyysisen laitteiston muiden kanssa ja myös luottamaan datansa ja yksityisyytensä palveluntarjoajan käsiin. Pilvipalveluiden eriävät ominaisuudet verrattaessa perinteiseen malliin siis itseasiassa luovat poikkeavat vaatimukset tietoturvaan. Seuraavaksi esitellään kuusi tietoturvavaatimusta ja mikä niiden merkitys on pilvipalveluissa.

Saatavuutta pidetään yhtenä pilvipalveluiden avainelementeistä. Pilvipalveluita käytetään pilvipalvelumallista huolimatta jonkin verkon yli, joten asiakkaan ostamasta palvelusta ei ole mitään arvoa, jos se ei ole saatavilla jatkuvasti. Sopimuksessa on yleensä määritelty jonkin asteinen palvelutaso, esimerkiksi 99,9%. On tärkeää, että myös asiakas on tuntee sopimusvelvoitteet, koska esimerkiksi ehtoja rikottaessa tai maksun myöhästyessä on mahdollista, että palveluntarjoaja sulkee palvelun ja asiakas menettää datansa. (Cachin ym., 2009.)

Luottamuksellisuudella käsitetään, että asiakkaan lähettämää dataa ja tietoja pidetään salassa tallennuksen ja siirron aikana. Luottamuksellisuuden puutetta on pidetty pilvipalveluiden aihealueella yhtenä merkittävimmistä huolenaiheista. Palveluntarjoajan on helppo päästä käsiksi asiakkaan tallentamaan dataan, joten asiakkaan on tärkeää pystyä luottamaan palveluntarjoajaan. Myös kolmansien osapuolten hyökkäykset on otettava huomioon. Asiakkaan pitää pystyä luottamaan palveluntarjoajaan, ettei kolmas osapuoli pääse missään tilanteessa käsiksi asiakkaan tallentamaan dataan. Palveluntarjoaja ei kuitenkaan ole yksin täysin vastuussa kolmansien osapuolten urkinnasta. Asiakas voi myös itse omalla toiminnallaan esimerkiksi paljastaa salasanansa, jolloin mahdollisesti syntyvästä tietoturvauhasta on vastuussa asiakas itse, eikä palveluntarjoaja. Cachin ym; (2009) mukaan luottamuksellisuutta on mahdollista parantaa esimerkiksi käyttämällä erilaisia salausmenetelmiä datan tiedonsiirrossa ja varastoinnissa. Näitä salausmenetelmiä kutsutaan kryptografisiksi avaimiksia ja niitä ei tule säilyttää samassa palvelussa, missä käyttäjän data sijaitsee.

Eheydellä tietoturvan alueella tarkoitetaan tietojen oikeellisuutta ja niiden paikkansa pitävyyttä. Eheydellä on pilvipalveluissa tärkeä asema, koska tiedonsiirto asiakkaalta palveluntarjoajan datakeskuksiin tapahtuu oletusarvoisesti aina epäluotettavaa verkkoa pitkin. Ohjelmistovirheet ja epäluotettava verkkoyhteys voi aiheuttaa tiedostojen vioittumisen siirtovaiheessa. Asiakkaan pitää pystyä myös tässä tapauksessa luottamaan siihen, ettei kolmas osapuoli pääse oikeudettomasti käsittelemään tiedostoja verkkolevyllä. Eheyteen liittyviä ongelmia voidaan pyrkiä esimerkiksi ratkaisemaan digitaalisilla allekirjoituksilla ja tiivistealgoritmeillä.(Cachin ym., 2009.)

Pääsynvalvonta tarkoittaa, että palveluntarjoajan palveluiden käyttäjiä ja heidän käyttöoikeuksiaan voidaan hallinnoida ja että käyttäjät voidaan tunnistaa. Pääsynvalvontaa yleensä kontrolloidaan käyttäjätunnuksen ja salasanan tai erilaisten kryptografisten avainten avulla. Pääsynvalvonnan kontrollointi pilvipalveluissa on tärkeää, koska käyttäjillä palvelussa voi olla erilaisia käyttöoikeuksia ja myös palvelu voi sisältää eri käyttäjillä henkilökohtaisia tiedostoja ja tietoja. (Cachin ym., 2009.)

Hallinnalla tarkoitetaan, että käyttäjän täytyy pystyä hallinnoimaan infrastruktuurin mahdollistamia resursseja reaaliajassa. Käyttäjällä täytyy siis olla oikeus palvelun tilan ja näkyvyyden kontrollointiin. Palvelun hallinnointi tapahtuu yleensä jonkinlaisen rajapinnan kautta. Hallinta tarkoittaa

käytännössä esimerkiksi sitä, että käyttäjän täytyy pystyä poistamaan tiedostoja palvelimelta tai tarvittaessa ajamaan verkkopalvelu alas.(Cachin ym., 2009.)

Seurannan avulla käyttäjä voi seurata yksityiskohtaisesti infrastruktuurin tilaa ja saada tietoa tästä reaaliajassa. Käyttäjä voi saada tietoa esimerkiksi verkon kuormitusasteesta tai levytilan käyttöasteesta. (Cachin ym., 2009.)

3.2 Tyypilliset tietoturvaongelmat pilvipalveluissa

Pilvipalveluiden tietoturvaongelmat voidaan jakaa karkeasti kahteen luokkaan: ulkoiset ja sisäiset. Ulkoisilla riskeillä tarkoitetaan ns. perinteisiä tietoturvaongelmia, joita kaikki verkkoon kytketyt tietokoneet voivat kohdata. Sisäisillä riskeillä tarkoitetaan pilvipalvelusta itsestään johtuvia uhkia. Tietoturva pilvipalveluissa voidaan jakaa kolmeen pääkategoriaan, joihin uhat voidaan luokitella. Nämä ovat myös suurimmat huolenaiheet asiakkaalla pilveen siirryttäessä. Nämä kategoriat ovat: yleinen tietoturva, saatavuus ja kolmas osapuoli(Chow ym., 2009). Tässä alaluvussa käsitellään nämä pilvipalveluille spesifit kategoriat ja niissä ilmenevät tietoturvaongelmat. Ratkaisuja ilmeneviin ongelmiin esitellään luvussa neljä.

3.2.1 Yleinen tietoturva

Yleisen tietoturvan vaatimuksena on, että asiakkaan data säilyy muuttumattomana ilman, että mikään kolmas osapuoli ei pääse sitä muokkaamaan tai poistamaan. Carrollin, Merwen ja Kotzen (2011) mukaan, koska pilvipalveluissa ohjelmistot tarjotaan palveluina, joita palveluntarjoajat ylläpitävät, ei tietojen hallinnointi ole loppukäyttäjän hallussa. Yleiseen tietoturvaan pilvipalveluissa määritellään kuuluvaksi tiedon eheys, oikeellisuuden turvaaminen ja pääsynvalvonta. (Chow ym., 2009).

Yritysten ja organisaatioiden kannalta pilvipalvelut tuovat merkittävän riskin. Pilvipalveluissa ohjelmistot on jaettu monen organisaation käyttöön, jolloin samoilla palvelimilla on useiden eri organisaatioiden tietoja. Tämä tuo mukanaan riskin, että organisaation tiedot joutuvat esimerkiksi kilpailijan käsiin. (Viega, 2009). Organisaation toiminnasta riippuen, tietokannat saattavat sisältää paljon yksityistä informaatiota asiakkaista, esimerkiksi sosiaaliturvatunnuksia. Tällaisten tietojen joutuminen ja leviäminen kolmansien osapuolten käsiin voi olla todella vaarallista.

Myös tietojen kalastelua(engl. phishing) pidetään merkittävänä riskinä, koskien tietoturvaa. Tietojen kalastelijat voivat kiinnostua palvelimista, joissa säilytetään useiden eri organisaation tietoja, sen sijaan, että kalastelu suuntautuisi vain organisaatioiden palvelimille. (Chow ym., 2009.) Tietovuodot ja tietojen kalastelu eivät ole kuitenkaan pelkästään pilvipalveluiden haavoittuvuuksia, vaan niitä esiintyy myös perinteisimmissä organisaatioiden IT-ratkaisuissa. Pilvipalveluiden tietovuodoissa on vain paljon suurempi

vaikutus kuin perinteiseen IT-infrastruktuuriin kohdistuvassa hyökkäyksessä. (Chow ym., 2009.)

3.2.2 Saatavuus

Toisena riskinä pilvipalveluissa voidaan pitää luvussa 3.1 esiteltyä saatavuutta. Saatavuus myös voidaan nähdä hyötynä. Koska pilvipalvelut ovat hajautettuja järjestelmiä, on mahdollista, että käyttäjän tieto sijaitsee useilla palvelimilla ja mahdollisesti myös eri mantereilla. Kun tieto on hajautettu se mahdollistaa hyvän saatavuuden ja virheensietokyvyn. Käytännössä tämä merkitsee sitä, että yhden palvelimen rikkoutuessa koko palvelu ei kuitenkaan kaadu. On kuitenkin mahdollista, että palveluntarjoaja kohtaa järjestelmävirheen, joka kaataa koko palvelun. Loppukäyttäjän kannalta tämä vaarantaa tietojen saatavuuden. Järjestelmävirhe ei välttämättä pelkästään kaada vain palvelua, mutta voi myös vahingoittaa käyttäjän tietoja. Tämän vuoksi säännöllinen varmuuskopiointi on hyvä keino asiakkaan turvautua tälläisiltä ongelmilta. (Armbrust ym., 2010.)

Tietojen lukkiutumisriski liittyy myös saatavuuteen. Lukkiutumisriski tarkoittaa, että eri palveluntarjoajien palvelut eivät ole vielä standardimuodossa. käyttäjän kannalta tämä hankaloittaa tietojen ja ohjelmistojen siirtämistä toiselle palveluntarjoajan palvelimelle. (Armbrust ym., 2010.) Armbrust ym. (2010) toteavat myös, että lukkiutumisen riskinä voi olla myös palveluntarjoajan poistuminen kokonaan markkinoilta, jolloin palvelun käyttäjälle ei jää tiedostojen ja ohjelmistojen kannalta muuta vaihtoehtoa kuin aloittaa uudestaan. Lukkiutumisriski on aina mahdollista, kun tietojen hallinta on kolmannen osapuolen vastuulla.

3.2.3 Kolmas osapuoli

Kolmannella osapuolella pilvipalveluissa tarkoitetaan pilvipalveluiden tarjoajaa. Kun asiakas ottaa käyttöönsä pilvipalvelua siirtää hän tietonsa ja datansa ulkopuolisen tahon käsiin ja luovuttaa tietojen hallinnan oman kontrollinsa ulottumattomiin. Kyseinen kontrollin menetys ja läpinäkyvyyden puute pilvipalveluissa lisää tietoturvaongelmia ja epävarmuutta palvelua kohtaan.(Chow ym., 2009.)

Chow ym. (2009) pitävät läpinäkyvyyden ongelmina varmuuden saamista asiakkaan tallennetun tiedon luotettavasta käsittelystä ja heikoista mahdollisuuksista varmistua tiedon tallennuksesta, koska asiakkaalla on mahdollisuus päästä tarkastamaan tallentamiaan tietoja vain dokumentaatiosta ja manuaalisella auditoinnilla.

Myös alihankintaketjut aiheuttavat ongelmia tietoturvassa. Palveluntarjoaja voi itse käyttää toiminnassaan alihankkijoita, jolloin käyttäjä on alihankintaketjun alapäässä. Tämä vähentää entisestään asiakkaan kontorollia dataan ja myös laskee luottamusta.(Chow ym., 2009.)

3.3 Esimerkkejä käytännön tietoturvaongelmista

Tämän alaluvun tarkoitus on antaa esimerkkejä toteutuneista tietoturvaongelmista eri palveluntarjoajien kohdalla. Esimerkkien on tarkoitus selventää rajapintaa teorian ja käytännön välillä. Ratkaisuja tietoturvaongelmiin esitellään luvussa 4.

Ensimmäinen tapaus sattui pilvipalveluntarjoajalle LinkUp, joka kadotti 45% tallennetusta asiakasdatasta järjestelmänvalvojanvirheen vuoksi. Tämä tapaus johti suoraan palveluntarjoajan liiketoiminnan kaatumiseen. Tapauksen johdosta myös kävi ilmi, että asiakkaiden vanha data ja varmuuskopioinnit ovat kallis kulu palveluntarjoajalle. Tämä on johtanut siihen, että jotkut palveluntarjoajat ovat ryhtyneet säilömään osaa asiakkaan datasta kolmasilla osapuolilla.(Cachin, Keidar, Shraer, 2009.) Tämä on palveluntarjoajan kannalta hyvä keino vähentää taakkaa ja vapauttaa resursseja, mutta se vähentää luottamuksellisuutta palveluntarjoajan ja asiakkaan välillä.

Palveluntarjoaja tarjoaa palvelun saatavuutta ympärivuorokautisesti, mutta palvelukatkokset ovat merkittävä ongelma pilvipalveluissa. Esimerkiksi palvelukatkokset Google Mail, Hotmail, Amazon S3 ja MobileME –verkkopalveluissa aiheuttivat mittavia ongelmia palveluntarjoajalle ja käyttäjille (Cachin ym., 2009).

Luvaton asiakkaiden datan tarkastelu ja käyttö ei aina ole kolmannen osapuolen tai hakkerin aiheuttama, vaan se voi johtua myös ohjelmistovirheestä palveluntarjoajan palvelussa. Esimerkiksi tällainen ohjelmistovirhe tapahtui Google Docs –palvelussa vuonna 2009. Myös Amazonin S3 –palvelussa tapahtui palveluntarjoajan ohjelmistovirhe, joka aiheutti asiakkaiden datan korruptiota.(Cachin ym., 2009.)

4 Tietoturvaratkaisut pilvipalveluissa

Tutkimuksen edellisessä luvussa käytiin läpi yleisiä tietoturvaongelmia pilvipalveluissa. Näihin ongelmiin on teoriassa ja käytännössä kehitetty ratkaisuja, joita tutkielman tämän luvun tarkoitus on käydä läpi. Ensiksi läpi käydään kaksi tietoturvamallia, jotka ovat kehitetty parantamaan pilvipalveluiden tietoturvaa, sekä lisäämään luottamuksellisuutta palveluntarjoajan ja käyttäjän välillä. Tietoturvamallit käydään tutkimuksessa läpi toimintaperiaatetasolla, eikä niiden tekniseen toteutukseen perehdytä kovin tarkasti. Tämän jälkeen luvussa perehdytään yleisiin tietoturvaratkaisuihin pilvipalveluissa.

4.1 Tietoturvamallit pilvipalveluissa

Tässä alaluvussa esitellään kaksi teoreettista mallia, joiden tarkoitus on ratkaista luottamusongelma pilvipalveluissa, sekä parantaa tietoturvaa. Ensimmäiseksi esitellään Trusted Cloud Computing Platform eli TCCP (Santos, Gummadi & Rodrigues, 2009). Tämä on alusta, jolla pyritään ratkaisemaan luottamusongelma asiakkaan ja palveluntarjoajan välillä. TCCP-alustalle on tarkka määritelmä, jonka pohjalta voitaisiin luoda myös ohjelmistoteutus.

Toinen malli on nimeltään SecureCloud (Takabi, Joshi & Ahn, 2010), joka on teoreettinen malli, eikä spesifikaatio niin kuin TCCP. SecureCloud-mallin tarkoitus on integroida useita pilvipalveluita yhdeksi loogiseksi ja toimivaksi järjestelmäksi. Tässä tutkimuksessa kumpaankaan malliin ei kuitenkaan perehdytä, vaan ainoastaan esitellään niiden perustoimintaperiaate.

4.1.1 TCCP

Ensimmäinen esiteltävä tietoturvamalli on nimeltään TCCP (Trusted Cloud Computing Platform). Mallin tarkoitus on ratkaista luottamusongelma asiakkaan ja palveluntarjoajan välillä. Malli on kehitetty erityisesti IaaS-

palvelumallia varten. Oletus on, että palveluntarjoajan järjestelmäylläpitäjällä on pääsy kaikkiin tietokoneisiin, joilla asiakkaan virtuaalikoneita ajetaan. Täten voidaan ajatella, että ylläpitäjä voi melko helposti käyttää väärin käyttöoikeuksiaan.(Santos ym., 2009.) TCCP:n toimintaperiaatteena on, että se tarjoaa niin sanotun suljetun laatikon ajoympäristön(engl. closed box execution enviroment) virtuaalikoneille. Tällä pyritään varmistamaan, ettei järjestelmän ylläpitäjä pääse käyttöoikeuksillaan muokkaamaan tai tarkastelemaan virtuaalikoneiden sisältöä. TCCP-malli myös mahdollistaa asiakkaan tarkistaa, että palvelu käyttää TCCP-mallia ja on siten myös turvallinen. (Shen, Li, Yan & Wu, 2010.)

TCCP-mallin toteutuksen kannalta oleellisimmat komponentit ovat TVMM(trusted virtual machine monitor) ja TC(trusted coordinator). Logiikka näiden komponenttien toiminnassa on, että TVMM sijaitsee jokaisella pilvipalvelun fyysisellä palvelimella, josta asiakkaan virtuaalikoneita ajetaan. TVMM:n tarkoitus on monitoroida ja varmistaa, että fyysisesti koneille pääsevä ylläpitäjä ei näe virtuaalikoneiden sisältöä ja täten varmistaa paikallinen turvallisuus. (Santos ym., 2009.)

Toinen TCCP-mallin kannalta oleellinen komponentti on TC. TC:n tehtävä mallissa on pitää kirjaa luotetuista palvelimista. TC varmistaa jokaiselta palvelimelta, että siellä ajetaan asianmukaisesti edellisessä kappaleessa esitettyä TVMM-monitoria. Palvelun käyttäjä voi varmistaa, että palvelin, jolta hänen virtuaalikoneita ajetaan on luotettava ja tietoturvallinen. TC-komponentti voi poistaa tai lisätä dynaamisesti palvelimia luotettujen palvelinten listalta. (Lombardi & Di Pietro, 2011.)

Viimeisimpänä TCCP-mallin kannalta olennainen käsite on ETE(external trusted entity). ETE on pilvipalveluntarjoajasta erillään oleva toimija, joka ylläpitää TC:tä. ETE-toimijan, jonka tehtävänä on valvoa IaaS-palvelua riittävästi, jotta se voi varmistua siitä seikasta, että asiakkaiden virtuaalikoneet ovat riittävästi suojattuja. ETE käyttää komunikointiin eri tahojen kanssa kryptografisia avaimia, joiden tarkoitus on turvata identiteetti. (Santos ym., 2009.)

Tärkeintä koko alustassa on, että pilvipalveluntarjoajilla ja niiden henkilöstöllä ei ole itse pääsyä ETE-järjestelmään lainkaan. Tämä on tärkeää turvallisuuden määritelmän takaamiseksi. Santos ym.(2009) ehdottavatkin, että ETE-järjestelmää hallinnoisivat erikseen määritellyt, luotetut tahot, kuten sertifikaatin saaneet tietoturvayritykset.

TCCP:n idea tiivistettynä on, että pilvipalvelua ajetaan sellaisella alustalla, että asiakkaalla on mahdollisuus varmistua virtuaalikoneensa turvallisuudesta. Sertifioitu ja luotettava kolmas osapuoli koordinoi dynaamisesti luotettaviksi todettuja palvelimia ja täten vahvistaa asiakkaalle palvelun turvallisuuden.

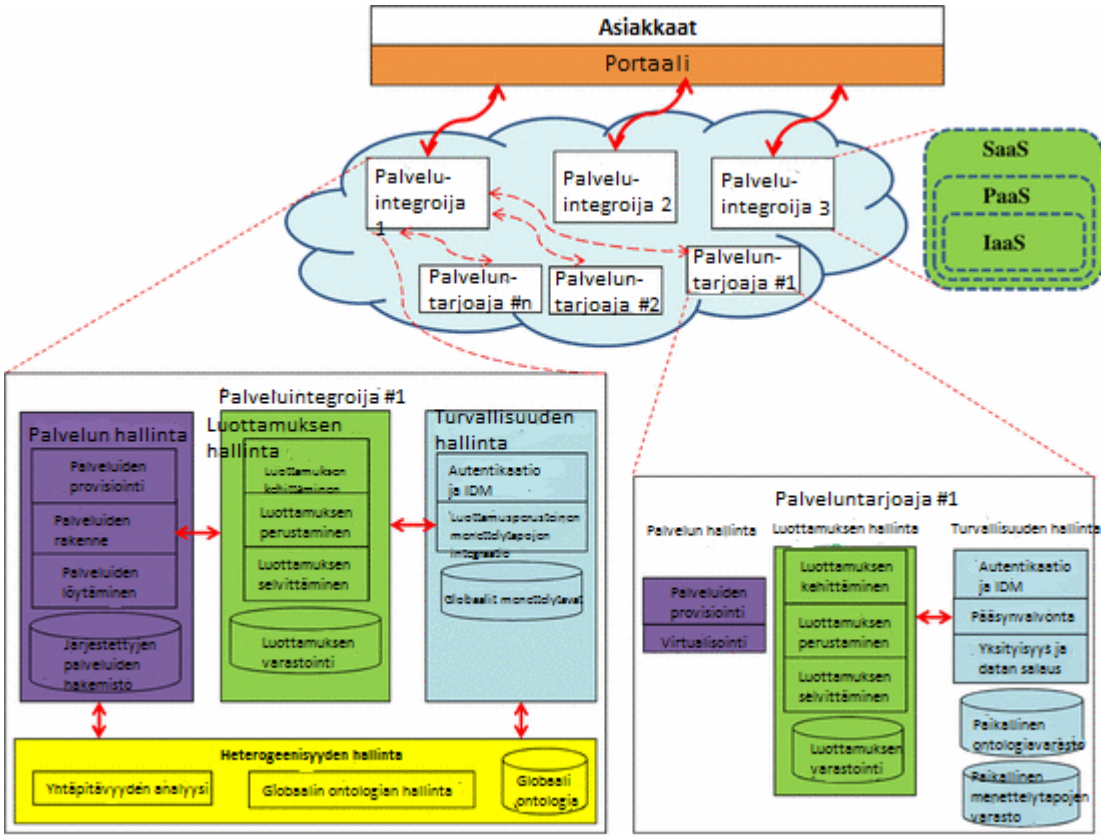
4.1.2 SecureCloud

Toinen esiteltävä malli on nimeltään SecureCloud. Takabi ym. (2010) ovat luoneet artikkelissaan teoreettisen mallin, jonka avulla asiakasorganisaatio voi muodostaa toimivan, turvallisen ja yhtenäisen järjestelmän. Lähtökohtana kehittämiselle oli muodostaa toimiva järjestelmä organisaatioille ja yrityksille, jotka tarvitsevat toimintaansa palveluja monelta eri pilvipalveluntarjoajalta. SecureCloud on tietoturvamalli, joka pyrkii integroimaan pilvipalveluja yhteen ja täten muodostaa turvallisen ja luotettavan mallin. SecureCloud on ainoastaan teoreettinen malli siitä miten voidaan ratkaista useiden pilvipalvelutarjoajien palveluiden integrointiongelmat organisaation sisällä.

Takabi ym. (2010) näkevät pilvipalvelujen integroinnissa kaksi ongelmakohtaa. Ensimmäinen ongelmakohta on eri palveluiden erilaiset tietoturvapolitiikat. Nämä eivät ole yleensä keskenään yhteensopivia. Yhteensopivuus täytyy varmistaa, että palveluiden tietoturvavaatimukset kohtaavat ja jokainen taho noudattaa niitä. Lisäksi useiden pilvipalveluiden integroinnissa tulee vastaan kommunikointiongelma. Kommunikointi eri pilvipalveluiden välillä on tärkeää hoitaa turvallisesti ja luotettavasti.

Toinen ongelma on käyttäjien tunnistautuminen, hallinta ja pääsynvalvonta. Ei ole käytännöllistä, että esimerkiksi yrityksen sisällä jokaisella työntekijällä on erilliset tunnukset eri järjestelmiin. Tämän sijaan tunnistautuminen ja pääsynvalvonta on helpointa, että jokaisella käyttäjällä olisi yksi oma tunnus ja tämän perusteella pitäisi olla automaattisesti pääsy kaikkiin palveluihin, johon käyttäjän käyttöoikeudet riittävät. (Takabi ym., 2010.)

Takabin ym. (2010) mukaan ratkaisuksi näihin ongelmiin on SecureCloud ympäristössä integrointikomponentti nimeltään palveluintegroija(eng. service integrator). Integrointikomponentti sisältää kaikki tarvittavat moduulit palvelun, turvallisuuden ja luottamuksen hallintaan. Jokaisesta pilvipalvelusta löytyvät loogiset vastaavat moduulit. Näin useasta pilvipalvelusta saadaan yhtenäinen portaali.



Kuvio 2 Tietoturvakehys pilvipalveluympäristölle

Integrointikomponentin tehtävä on tulkita palvelu käyttäjilleen siten, että palvelut ovat tietoturvaominaisuuksiltaan yhteneväisiä, pääsynhallinta toimii suoraan ja ettei käyttäjien tarvitse huolehtia jokaisen palvelun turvallisuudesta erikseen.(Takabi ym., 2010.)

4.2 Ratkaisuja tietoturvaongelmiin

Tämän luvun tarkoitus on vastata tutkielman luvussa kolme esitettyihin pilvipalveluiden tietoturvariskeihin. Uudet palvelut ja niihin siirtyminen tuovat mukanaan haasteita. Nämä haasteet organisaation tulee ottaa huomioon pilvipalveluita harkittaessaan. Luvussa kolme esitellyt haasteet ovat seuraavat: yleinen tietoturva, tiedon saatavuus ja kolmannen osapuolen tiedonhallinta. Nämä asiat voidaan katsoa hyödyn lisäksi haasteina.(Chow ym., 2009.) Tosin pilvipalveluiden kanssa kohdataan paljon samoja haasteita kuin perinteisen IT-ympäristön kanssa(Brunette & Mogull, 2009).

Pilvipalvelujen täysimääräinen hyödyntäminen edellyttää yksityisyyteen ja tietoturvaan liittyvien asioiden huomioonottamista arkaluontoisen tiedon

ollessa hajallaan eri puolilla Internetiä. Pilvipalveluiden tapauksessa on tärkeää ymmärtää, että hajautetut järjestelmät ovat turvallisuudeltaan heikompia kuin esimerkiksi yrityksen sisäinen tietojärjestelmäarkkitehtuuri (Kaufman, 2009). Pilvipalveluihin siirryttäessä on myös huomionarvoista, että pilvipalvelun tilaavalla taholla tulisi olla mahdollisuus määrittää menetelmiä liittyen tietoturvaan ja riskienhallintaan, jotka ovat yhteneväisiä yrityksen päämäärien ja operatiivisen riskienhallinnan kanssa (Kaufman, 2009).

Tiedon saatavuuteen liittyy myös ongelmia, jos esimerkiksi pilvipalveluita tarjoava yritys lopettaa toimintansa. Tiedon saatavuus onkin ensisijaisen tärkeä pilvipalvelun turvallisuuden kannalta. Kandukur, Paturi & Rakshit (2009) ehdottavatkin, että palveluntarjoajan muuttuessa tulisi tiedon saatavuus määritellä palvelutasosopimuksissa. Pilviteknologiaa kuitenkin jo kehitetään ennen palvelusopimusten laatimista, siksi jo pilvipalveluita kehittäessä tulisi ottaa huomioon tiedon saatavuus. Saatavuutta voidaan myös parantaa tiivistämällä yhteistyötä eri palveluntarjoajien välillä, siksi pilven arkkitehtuureja suunniteltaessa tulisi ottaa huomioon pilvien välinen liitettävyys. (Sripanidkulchai, Sahu, Ruan, Shaikh & Dorai, 2010.)

Tiedon tallentaminen, sekä tiedon liikkuminen järjestelmien välillä on yleisen tietoturvallisuuden kannalta tärkeitä alueita. Tietojen tallennuksen ja säilytyksen suojaamiseen voidaan käyttää erilaisia pirstaloimismenetelmiä, jolloin tieto hajautetaan eri palvelimille. Tiedon liikkumista voidaan suojata myös samalla tavoin kuin tallennusta, mutta sitä voidaan myös vahvistaa käyttämällä erilaisia salausmenetelmiä.(Samarati & di Vimercati, 2010.)

Yksityisyyden kannalta merkittävä tietoturvauhka on palvelinten tietokantoihin tehtävät haut ja erityisesti niiden indeksointi. Hakujen indeksointien tehokkuus on ongelmallista yksityisyyden näkökulmasta. Toistaiseksi on vasta pystytty kehittämään erilaisia metodeja, joissa tehokkaiden indeksointien edellytyksenä voi olla yksityisyyden vaarantuminen. Tietoturvauhka on myös olemassa, jos tietokantakyselyjen salassapito on vaarassa. (Samarati & di Vimercati, 2010.)

Samaratin & di Vimercatin (2010) mukaan hajautettujen järjestelmien pääsynvalvontaan voi liittyä riskejä, jos tieto menetelmästä, jolla tietoon pääsee käsiksi on arkaluontoista. Toisena ongelmana Samarati & di Vimercatin (2010) mukaan voidaan pitää tilannetta, jos tieto palvelimella edellyttää tiettyä valtuutustasoa ja johon palvelimella itsellään ei ole oikeuksia päästä käsiksi. Pääsynvalvontaa voidaan hallita erilaisilla todentamismenetelmillä, joissa käyttäjälle jaettavat oikeudet voivat perustua käyttäjän rooliin, tehtävään tai projektiin organisaatiossa (Chen, Hu, Du, Zhou & Ji, 2009).

Tiedon eheyden ja oikeellisuuden turvaamiseksi Samarati & di Vimercati (2010) ehdottaa palvelinta, joka ei voi nähdä itse tiedon sisältöä, mutta on silti luotettava käyttäjän käyttäjän tekemissä tietokantakyselyissa. Usein tietoa tuottavan käyttäjän todentaminen tapahtuu digitaalisten allekirjoitusten avulla (Samarati & di Vimercati, 2010).

Saatavuus ja kolmannen osapuolen läsnäolo ovat hyötyjen lisäksi selviä riskejä organisaatiolle pilvipalveluissa. Pilvipalveluiden tietoturvan kannalta

tärkeimpiä turvattavia asioita ovat eheys, käytettävyys, luottamuksellisuus, sekä pääsynvalvonta.

5 Yhteenveto ja pohdinta

Tutkimuksessa käsiteltiin pilvipalveluita, niiden tietoturvaongelmia ja ratkaisuja näihin tietoturvaongelmiin. Tämä kirjallisuuskatsauksena toteutettu tutkimus etsi vastauksia seuraaviin tutkimuskysymyksiin: ”Mitä ovat pilvipalvelut?”, ”Millaisia ovat erilaiset pilvipalveluissa kohdattavat tietoturvariskit?” ja ”Miten pilvipalveluiden turvallisuutta voidaan parantaa loppukäyttäjän kannalta?”.

Tutkimuksen toisessa luvussa käytiin läpi pilvipalvelut-käsitettä ja esiteltiin mistä pilvipalvelut koostuvat. Luku vastaa ensimmäiseeen tutkimuskysymykseen. Käsiteltäviä asioita olivat pilvipalvelumallit: julkinen- , yksityinen- ja hybridipilvi. Myös pilvipalvelumallit käytiin läpi, joita ovat: IaaS, PaaS ja SaaS. Ensimmäisessä luvussa esiteltiin myös pilvipalveluiden tunnusomaiset ominaisuudet.

Tutkimuksen kolmas luku keskittyy pilvipalveluiden tietoturvaongelmiin. Luvussa ensiksi käytiin läpi reaalimaailmassa esiintyneitä tietoturvaongelmia pilvipalveluiden kentältä. Tämän jälkeen läpi käytiin pilvipalveluiden yleiset tietoturvavaatimukset, jossa myös sivuttiin niiden eroavaisuuksia perinteisiin tietoturvavaatimuksiin. Viimeinen läpikäyty asia luvussa oli pilvipalveluiden tietoturvaongelmat. Tietoturvaongelmat käytiin läpi yleisimpien esiintyvien ongelmien näkökulmasta. Toinen sisältöluku vastaa toiseen tutkimuskysymykseen. Tutkimusten valossa suurimmat huolta aiheuttavat tietoturvaongelmat pilvipalveluissa ovat: yleinen pilvipalvelun tietoturva, palveluiden saatavuus ja kolmannen osapuolen rooli pilvipalveluissa.

Neljäs luku keskittyi pilvipalveluiden tietoturvaongelmien ratkaisuihin. Ensiksi luvussa esiteltiin muutama tietoturvamalli, joiden tarkoitus on parantaa erityisesti pilvipalveluiden tietoturvaa. Tämän jälkeen luvussa esiteltiin ratkaisuja tyyppilisimpiin tietoturvaongelmiin pilvipalveluissa, joita tutkimuksen toinen sisältöluku kävi läpi. Luku vastaa viimeiseen tutkimuskysymykseen. Pilvipalveluiden tietoturvan kannalta eheys, käytettävyys, luottamuksellisuus ja pääsynvalvonnan hallinointi on kehittämisen arvoisia asioita.

Lähteinä tässä tutkimuksessa käytettiin tieteellisiä lähteitä, pääasiassa lähteet koostuvat aihealuetta ympäröivistä konferenssi- ja lehtijulkaisuista. Myös Petteri Heinon kirjaa käytettiin tutkimuksen lähteenä ja myös ennen kirjoitusprosessin alkuna aihealueeseen tutustuttavana teoksena.

Jatkotutkimuksena olisi mielestäni hyödyllistä tutkia, kuinka tässä tutkimuksessa esitellyt tietoturvaongelmat esiintyvät todellisuudessa, ja miten yritykset varautuvat näihin ongelmiin. Olisi myös jatkotutkimuksen kannalta konkreettista tutkia yritystä, joka on joutunut pilvipalveluihin siirryttäessä kohtaamaan jonkin vakavan tietoturvaongelman.

LÄHTEET

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

Brunette, G., & Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing v2. 1. *Cloud Security Alliance*, 1-76.

Cachin, C., Keidar, I., & Shraer, A. (2009). Trusting the cloud. *Acm Sigact News*, *40*(2), 81-86.

Chen, D., Hu, R., Du, Z., Zhou, Z., & Ji, C. (2009, June). Research on an SOA-based virtual enterprise access control model. In *Industrial Informatics, 2009. INDIN 2009. 7th IEEE International Conference on* (pp. 871-874). IEEE.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009, November). Controlling data in the cloud: outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on Cloud computing security* (pp. 85-90). ACM.

Dillon, T., Wu, C., & Chang, E. (2010, April). Cloud computing: issues and challenges. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on* (pp. 27-33). Ieee.

Hayes B. Cloud computing. Commun. ACM, 51:9–11, July 2008. ISSN 0001-0782. doi: http://doi.acm.org/10.1145/1364782.1364786. URL http://doi.acm.org/10.1145/1364782.1364786.

Heino, Petteri. (toim.) 2010. Pilvipalvelut. Hämeenlinna, Talentum Media. 267 s.

Jansen, Wayne, and Timothy Grance. "Guidelines on security and privacy in public cloud computing." *NIST special publication* 800 (2011): 144.

B.R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing, pp.517-520

Kaufman, L.M. 2009. Data Security in the World of Cloud Computing. IEEE Security & Privacy Magazine 7(4), 61-64.

Li, Q., Wang, Z. Y., Li, W. H., Li, J., Wang, C., & Du, R. Y. (2013). Applications integration in a hybrid cloud computing environment: modelling and platform. *Enterprise Information Systems*, *7*(3), 237-271.

Lombardi, F., & Di Pietro, R. (2011). Secure virtualization for cloud computing.*Journal of Network and Computer Applications*, *34*(4), 1113-1122.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

PALLIS, George. "Cloud Computing: The New Frontier of Internet Computing."*IEEE internet computing* 14.5 (2010): 70-73.

Popovic, K., & Hocenski, Z. (2010, May). Cloud computing security issues and challenges. In *MIPRO, 2010 proceedings of the 33rd international convention*(pp. 344-349). IEEE.

Samarati, P., & di Vimercati, S. D. C. (2010, April). Data protection in outsourcing scenarios: Issues and directions. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security* (pp. 1-14). ACM.

Santos, N., Gummadi, K. P., & Rodrigues, R. (2009, June). Towards trusted cloud computing. In *Proceedings of the 2009 conference on Hot topics in cloud computing* (pp. 3-3).

Shen, Z., Li, L., Yan, F., & Wu, X. (2010, May). Cloud computing system based on trusted computing platform. In *Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on* (Vol. 1, pp. 942-945). IEEE.

Sripanidkulchai, K., Sahu, S., Ruan, Y., Shaikh, A., & Dorai, C. (2010). Are clouds ready for large distributed applications?. *ACM SIGOPS Operating Systems Review*, *44*(2), 18-23.

Takabi, H., Joshi, J. B., & Ahn, G. J. (2010, July). Securecloud: Towards a comprehensive security framework for cloud computing environments. In*Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual* (pp. 393-398). IEEE.

Viega, J. (2009). Cloud computing and the common man. *Computer*, *42*(8), 106-108.