LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Pilvipalveluiden tietoturvallisuus ja niiden edut sekä uhat

Laukkonen, Riku

2016 Laurea

Laurea-ammattikorkeakoulu

Pilvipalveluiden tietoturvallisuus ja niiden edut sekä uhat

Riku Laukkonen
Liiketalouden tradenomi
Opinnäytetyö
Kesäkuu, 2016

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutusohjelma
Liiketalouden ammattikorkeakoulututkinto

Riku Laukkonen

Pilvipalveluiden tietoturvallisuus ja niiden edut sekä uhat

Vuosi 2016 Sivumäärä 31

Tämän työn tarkoitus on selvittää pilvipalveluiden tekninen peruste ja syitä siirtyä niiden käyttöön perinteisten it-ratkaisuiden sijaan. Tavoitteena on ymmärtää näitä syitä ja selvittää pilven etuja ja mahdollisia haittoja verrattuna perinteisiin ratkaisuihin. Tavoitteena on myös selvittää pilven tuomia uhkia yksityisyydelle ja kuinka yksityisyyttä voidaan suojata.

Kehittämistehtävänä voidaan pitää näiden syiden selvittämisen tarjoamaa informaatiota. Informaatio auttaa pohtimaan, missä tilanteissa siirtyminen pilvipalveluihin on perusteltua. Viitekehyksenä on käytetty kirjallisia lähteitä e-kirjoista ja internetistä valikoituja lähteitä.

Menetelmänä on käytetty kirjallisten lähteiden analysointia ja raportointia. Keskeisinä tuloksina voidaan pitää, että pilvipalvelut ovat nykyaikaisia, säästävät kustannuksia ja nostavat yritysten tehokkuutta. Pilvipalveluiden ansiosta yritykset voivat ulkoistaa oman it-osastonsa ja keskittyä ydinosaamiseensa. Pilven suurin uhka on sen tuoma riski yksityisyydelle, jota voidaan suojata tarkalla kumppanin valinnalla ja vaatimalla heiltä sensitiivisen tiedon huolellista hallintaa.

Työssä saatiin hyvä yleiskäsitys pilviarkkitehtuurin teknisestä puolesta sekä pilven eduista. Johtopäätös on, että siirtyminen pilveen on hyödyllistä monessa suhteessa vaikka kaikkea tietoa ei pilveen kannatakaan siirtää. Kehittämisehdotuksena voidaan mainita tarkkojen kustannuslaskelmien hyöty pohdittaessa eri vaihtoehtoja oman yrityksen it-ratkaisuille.

Asiasanat: Pilvipalvelut, Tietoturva, Virtualisointi

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Riku Laukkonen

Information Security of Cloud Services and its benefits and disadvantages

Year 2016 Pages 31

The purpose of this thesis is to find out the technical foundation of cloud services and reasons to start using them instead of traditional IT solutions. The goal is to understand these reasons and define benefits and possible drawbacks of cloud services when compared with traditional solutions. Another goal is to find out possible threats to privacy and how to protect it.

The information gathered from these findings can be seen as a development goal. That information helps to understand when starting to use cloud services is justifiable. Printed books, e-books and reliable sources from the internet have been used as a framework.

Analysis and reporting of written sources has been used as a method. An essential outcome is that cloud services are modern, save costs and raise companies' efficiency. Because of cloud services companies can outsource their own IT-department and focus on their core-expertise. The biggest threat that cloud services bring is their threat to privacy which can be protected by choosing business partners accurately and by demanding that they handle sensitive information carefully.

A good general knowledge of the technical side of cloud services and their benefits was achieved in this thesis. The conclusion is that starting to use cloud services is beneficial in many ways although not all information should be transferred to the cloud. The benefit of accurate cost calculation while discussing different options to the company's it-solutions can be seen as a development proposal.

Keywords: cloud services, information security, virtualization

Sisällys

1 Johdanto 6
2 Pilvipalveluiden käsitteet 6
3 Syitä pilvipalveuiden yleistymiselle 11
3.1 Virtualisointi 13
3.2 Tallennustilan virtualisointi 14
4 Pilvipalveluiden taloudelliset edut 15
5 Pilvipalveuihin kohdistuvat uhkatekijät 17
5.1 Uhat yksityisyydelle 21
5.2 Uhat infrastruktuurille, datalle ja pääsynhallinnalle 23
6 Pilvipalveluiden turvaaminen 25
6.1 Tiedon turvaaminen pilvessä 26
6.2 Turvamenettelyt datan suojaamiseksi 28
Lähteet 31

1 Johdanto

Opinnäytetyö käsittelee pilvipalveluiden tietoturvallisuutta ja pilvipalveluita yleisesellä tasolla. Työssä käsitellään seuraavia kysymyksiä: miksi pilvipalvelut kasvattavat jatkuvasti suosiotaan sekä ammattilaisten että tavallisten kuluttajien keskuudessa, pilvipalveluiden eri tekniset toteutustavat, pilvipalveluiden historia – mitä uutta ne tuovat tietotekniikan kentälle. Pilvipalvelut herättävät myös aiheellisesti suurta huolta käyttäjien yksityisyydestä ja myös tähän pyritään saamaan näkökulmaa sen hyödyistä ja haitoista: onko yksityisyyden väheneminen tai jopa menettäminen perusteltavissa palveluista saadulla hyödyllä. Työ on ajankohtainen pilvipalvelut käsitteen selventämiseksi. Työssä selvitetään myös, ovatko palvelut sopivia yritysten IT-ratkaisuiksi oman palvelutuotannon sijaan.

Pilvipalvelut ovat ajankohtainen ja kiinnostava aihealue IT-alalla. Pilvipalveluiden suosio on kasvanut ja tietoturvan merkitys on korostunut. Yritykset säilyttävät tärkeää ja osin salassa pidettävää liiketoimintaan liittyvää dataa pilvessä, joten on tärkeää tutkia, miten dataa voidaan säilyttää pilvessä turvallisesti.

Pilvipalvelut herättävät myös aiheellisesti suurta huolta käyttäjien yksityisyydestä ja myös tähän pyritään saamaan näkökulmaa sen hyödyistä ja haitoista: onko yksityisyyden väheneminen tai jopa menettäminen perusteltavissa palveluista saadulla hyödyllä. Pyrin saamaan vastaukset kvalitatiivisilla menetelmillä. Työssä pyritään vastaamaan kysymyksiin, miksi yritykset siirtyvät pilvipalveluiden käyttäjiksi ja mitkä syyt johtavat pilvipalveluiden käyttämiseen.

Työn tulosten avulla pyritään etsimään perusteluja pilvipalvelujen käyttöön otolle tai pitää yllä omaa palvelutuotantoa. Perusteluissa verrataan hyöty- ja haittanäkökulmia pilvipalveluiden käyttöönotosta. Työssä tutkitaan myös mitä pilvipalvelut itseasiasiassa tarkoittavat, sillä se ei ole välttämättä terminä kaikista selvin suurelle yleisölle, vaikka todennäköisesti suurin osa ihmisistä käyttääkin pilvipalveluita tiedostamatta asiaa. Pilvipalvelut määritellään työssä myös käsitteenä kirjallisuuden avulla.

2 Pilvipalveluiden käsitteet

Ennen varsinaista aiheen käsittelyä on hyvä selventää muutamia käsitteitä, joita tässä työssä tullaan käsittelemään. Äsken mainittujen lisäksi pilvipalveluita voidaan tuottaa eri tuotantomalleilla, joita ovat: infrastructure as a service eli IaaS, platform as a service eli PaaS ja software as a service eli SaaS.

Julkinen pilvi tarkoittaa palvelua, joka on saatavilla julkisen verkon kautta. Nämä palvelut saattavat olla ilmaisia tai maksullisia. Ne ovat siis helposti kaikkien saatavilla. Yleensä niitä käytetään yksinkertaisesti internetselaimen välityksellä. Julkisiin pilvipalveluihin liittyy kuitenkin riskejä, koska käyttäjä ei tiedä missä ja miten hänen tietojaan säilytetään. Nämä

palvelut suunnataankin yleensä yksityisille kuluttajille, joiden tietoturvallisuusvaatimukset ovat vähäisempiä kuin yrityksillä. Hyvä esimerkki tällaisesta palvelusta on Google ja sen pilvessä toimivat tallennusratkaisut kuten Google Drive.

Yksityinen pilvipalvelu tarkoittaa palvelua, joka on vain jonkin tahon saatavissa ja palvelua tuotetaan tuon tahon tiettyjä tarpeita varten. Se suunnitellaan ja skaalataan tarkasti ja se on myös aina maksullista palvelua. Yksityiset pilvet voivat olla hyvinkin suuria palveluita, toisaalta kaikki pilvipalvelut voivat olla kuten juuri Google, ja niiden datan säilytys paikat sekä tavat tunnetaan monesti paremmin kuin julkisissa palveluissa. Yksityisiä palveluita voi operoida joko ulkopuolinen palveluntarjoaja tai sitä käyttävä taho itse.

Hybiridi pilvi on sekoitus eri pilvipalveluita. Osa palveluista voidaan tuottaa julkisen pilven avulla ja osa yksityisellä. Käytännössä tämä takoittaa, että osa palveluista voidaan tuottaa yrityksen omassa konesalissa jota yritys hallinnoi itsenäisesti ja osa palveluista voidaan ostaa ulkoistettuna palveluna talon ulkopuolelta. On myös mahdollista ostaa pilvipalveluita ulkoistettuna useilta eri palveluntarjoajilta.

Infrastructure as a service (IaaS) on palvelu, jossa yritykselle annetaan käyttöön fyysisiä laitteita tai nykyään useamminkin virtuaalisia laitteita joissa voidaan ajaa yrityksen tarvitsemia ohjelmistoja sekä palveluita. Virtuaalinen laite, vios, on fyysisen laitteen sisällä toimiva virtuaalinen ratkaisu, joka antaa mahdollisuuden ajaa laitteen sisällä useampia toimintoja. Virtuaalisuus antaa mahdollisuuden skaalata yksi fyysinen laite useamman asiakkaan käyttöön eikä yhdellä asiakkaalla ole pääsyä toisen asiakkaan tietoihin. Tietokone siis jakaa virtuaalisesti resurssejaan eri prosesseille. IaaS-palveluntarjoaja hallinnoi kaikkea infrastruktuuria ja asiakkaan vastuulle jää kaikki muut tuotannon elementit. Näihin voi kuulua käyttöjärjestelmä, ohjelmistot ja käyttäjän toiminta systeemissä (Sosinsky 2011, 10).

Platform as a service (PaaS) on alustaratkaisu, jossa asiakkaalle tarjotaan ohjelmisto -sekä laitealusta minkä päällä heidän on helpompi suunnitella ja kehittää omia ohjelmistojaan. Näitä palveluita käyttävät esimerkiksi ohjelmistosuunnitteluun suuntautuneet yritykset. PaaS tarjoaa virtuaalikoneet, käyttöjärjestelmät, ohjelmistot, palvelut, kehitysympäristöt ja kontrollirakenteet. Asiakas voi siten viedä ohjelmistonsa pilveen tai käyttää ohjelmistoja, jotka on ohjelmoitu käyttäen ohjelmointikieliä ja työkaluja joita pilvipalvelun tuottaja tukee. Palveluntuottaja on vastuussa infrastruktuurista, käyttöjärjestelmästä ja ohjelmistoista, jotka tekevät palvelusta mahdollista. Asiakkaan vastuulle jäävät asentaa ja hallinnoida omia ohjelmistojaan, jotka se vie pilveen. (Sosinsky 2011, 10).

Software as a service on ohjelmisto tai mahdollisesti tietokanta, joka myydään palveluna pilviratkaisuna. Ulkopuolinen palveluntarjoaja pitää huolen ohjelmistoalustasta ja laitteistosta jotta ohjelmisto toimii aina, kun sitä tarvitaan. Palveluntarjoaja myös asentaa ohjelmistot pilvipalveluun jolloin asiakkaalle jää vain ohjelmiston käyttäminen. SaaS on täydellinen käyttöympäristö ohjelmistoineen, hallinnoineen ja käyttöliittymineen. SaaS

mallissa ohjelmisto tarjotaan asiakkaan käyttöön yleensä webselaimen kautta käyttöliittymänä. Asiakkaan vastuu alkaa ja loppuu datan syöttämiseen ja hallinnointiin sekä käyttäjän toimien hallinnointiin. Kaikki ohjelmistosta aina infrastruktuuriin on palveluntarjoajan vastuulla (Sosinsky 2011, 10).

Yleensä palvelut ovat virtualisoitu. Täten käyttäjillä on aina haluamansa ja vaatimansa näkymä infrastruktuuriinsa, lisäksi ohjelmistoihin ei kohdistu systeemisiä riippuvaisuuksia tai rajoituksia. Tätäkin tärkeämpää on kuitenkin pilven skaalattavuus: jos ohjelmisto tarvitsee lisäresursseja, niitä voidaan lisätä helposti automaattisen prosessin avulla. Ohjelmistosuunnittelijoiden ei siis tarvitse investoida omaan tietokonearkkitehtuuriin, vaan voivat hankkia tarvitsemansa resurssit joustavasti ulkopuoliselta palveluntarjoajalta samalla kun keskittyvät yrityksensä liiketoimintaan (Baun, Kunze, Nimis, Tai 2011, 1.)

Pilvipalvelut tekevät siis asiakkaansa elämän helpommaksi, koska heidän ei tarvitse tehdä suuria investointeja laitteisiin. Myös vastuu järjestelmän toiminnasta siirtyy palvelun tuottajalle. Asiakkaat pystyvät keskittymään siihen mikä on heille tärkeintä, eli oman liikentoimintansa pyörittämiseen.

Pilvipalveluissa on ideana, että käytöstä maksetaan. Tarvittavat resurssit tajotaan käyttöön ja niistä pitää maksaa. Käyttämättömistä resursseista ei tarvitse myöskään maksaa. Pilvipalveluiden voidaan saavuttaa merkittäviä taloudellisia säästöjä joustavan hinnoittelunsa ja helppokäyttöisyytensä takia. Tietokonekapasiteetti, joka tarjotaan käyttöön käyttäjän pyynnöstä on valtaisa, mikä luo suuruuden voimaa erittäin hyvällä kapasiteetti-hinta suhteella (Baun, Kunze, yms. 2011, 1-2).

Pilvipalveluiden kritisoijat tarttuvat mielellään pilvipalveluiden vaaroihin. Näitä vaaroja on, että suuret palveluyritykset tarjoavat kaikki omaa pilviratkaisuaan hakiessaan kilpailuetua. Kaikki ratkaisut ovat omanlaisiaan eikä yleisiä standardeja ole, joten yleisesti voidaan todeta ettei palveluntarjoajan vaihtaminen ole helppo tehtävä. Lisäksi kritisoijat tarttuvat mahdollisiin turvallisuusriskeihin. Lähempi tarkastelu paljastaa, että nämä argumentit tähtäävät hyvin usein puolustamaan perittyjä oikeuksia perinteisiin datakeskuksiin. Tästä syystä, yleensä nuoret yritykset kuten start-upit, jotka eivät kärsi tällaisista riippuvuuksista ottavat hyödyn irti uudesta pilviteknologiasta. On kuitenkin olemassa jo ansioituneita yrityksiä, jotka ovat ottaneet käyttöön pilvipalveluita ja voivat jo saada merkittäviä tehokkuuden parannuksia. Paitsi, että yritykset jotka käyttävät jo julkisia pilvipalveluita, ne luottavat kasvavissa määrin myös omiin yksityisiin pilviin (Baun, Kunze, yms. 2011, 2).

Pilvipalveluilla on siis puolensa. Asiakas saa käyttöönsä suhteellisen edullisesti erittäin paljon tietokonekapasiteettia, mutta se voi herättää kysymyksiä palvelun turvallisuudesta. Monesti edut, varsinkin taloudelliset, ovat kuitenkin niin suuret, että yrityksen on kannattavaa siirtyä pilvipalveluiden käyttäjäksi. Turvallisuus näkökohtiin tullaan kiinnittämään tarkemmin huomiota myöhemmin tässä työssä.

Asiakkaan näkökulmasta on monia kohtia, jotka tukevat tuottavampaa ja juostavampaa työtä: ottamalla edun markkinoilla olevista vaihtoehdoista, it-palveluiden ostajat pystyvät saavuttamaan itsenäisyyden perinteisistä staattisista datakeskusoperoijista. Tässä kontekstissa pilvipalvelut synnyttävät luovaa tuohoa vanhojen rakenteiden korvautuessa uusilla (Baun, Kunze, yms. 2011, 1, 2).

”Pilvipalvelu on malli, jolla mahdollistetaan tarpeen vaatiessa tietoverkon kautta kätevä pääsy jaettuihin ja ryhmäytettyihin tietokoneresursseihin, (verkot, palvelimet, tallennustila, ohjelmat, palvelut) jotka ovat konfiguroitavissa sekä luotettavia. Nämä resurssit voidaan provisioida ja julkaista nopeasti minimaalisella asiakkaan hallinnoinnilla tai palveluntarjoajan toiminnalla” (Krutz R, Russel V 2010, 2).

Pilvipalvelut viittaavat ohjelmistoihin ja palveluihin, joita ajetaan hajautetulla verkolla käyttämällä virtualisoituja resursseja ja joihin päästään käsiksi tavallisilla verkkoprotokollilla sekä verkkostandadeilla. Sen erityinen notaatio on, että resurssit ovat rajattomia ja virtuaalisia, ja että fyysisten järjestelmien yksityiskohdat joissa ohjelmistoja ajetaan ovat piilotettuja käyttäjältä (Sosinsky 2011, 3).

Palvelumallit määrittelevät minkälaista palvelua asiakkaille tarjotaan. Parhaiten tunnetaan SaS, PaS ja Iaas. Palvelumallit on rakennettu toistensa päälle ja määrittelevät mitä palveluntarjoajan pitää tehdä ja mitkä ovat asiakkaan vastuita (Sosinsky 2011, 3).

Pilvipalvelut esittävät todellisen muutoksen järjestelmien toimittamiseen. Pilvipalveluiden massiivinen skaala tuli mahdolliseksi internetin suosion sekä joidenkin palveluyritysten kasvun myötä. Pilvipalvelut tekevät mahdolliseksi kauan halutun tavan käyttää tietopalveluita, mikä on käytöstämaksamista, loppumatonta skaalautuvuutta ja universaalisti saatavia järjestelmiä. Pilvipalveluiden tuottamisen voi aloittaa pienesti ja kasvaa suureksi nopeasti ja siksi pilvipalvelut ovat vallankumouksellisia, vaikka niiden takana oleva teknologia on vain kehitysaskel vanhasta. Kaikki ohjelmistot eivät kuitenkaan hyödy pilvipalveluista. Ongelmia voivat aiheuttaa latenssi eli verkkoviive ja turvallisuus sekä hallinnollinen yhteensopivuus (Sosinsky 2011, 3).

Pilvipalvelut käyttävät virtualisointia ja moderneja tietoverkkoja tarjotakseen dynaamisesti resursseja monenlaisina palveluina, jotka jaetaan elektronisesti. Tällaiset palvelut tulisi olla saatavilla luotettavasti ja skaalautuvasti, jotta monet käyttäjät voivat käyttää niitä joko vain pyynnöstä tai vain, kun sille on tarvetta. (Baun, Kunze, yms. 2011, 3).

Palveluntarjoajan näkökulmasta tämä tarkoittaa usein moniin asiakkuuksiin perustuvaa arkkitehtuuria ja käyttöön perustuvaa laskutusta. Pilvipalvelut voidaan määritellä terminä seuraavasti: ”käyttämällä virtualisoituja tietokone -ja tallennusresursseja sekä moderneja verkkoteknologioita, pilvipalvelut tarjoavat skaalautuvan ja verkkokeskeisen abstraktin it-infrastruktuurin sekä alustat ja ohjelmistot palveluina tarvittuna aikana. Nämä palvelut laskutetaan käyttöön perustuen”. Tämä määritelmä ei missään tapauksessa ota kantaa

tuotetaanko palvelut hajautetulla arkkitehtuurilla vai yhdellä suurella palvelimella kuten keskustietokoneella. Pilvipalvelut eivät ole siis sama asia kuin klusteroitu tietotekniikka, mikä käyttää aina hajautettua arkkitehtuuria. Tavallisesti pilvipalvelutkin tukeutuvat hajautettuun arkkitehtuuriin, mutta niiden hallinta tapahtuu keskusjohtoisesti yhden palveluntarjoajan toimesta. Tämä on myös erona klusteroituun tietotekniikkaan, missä palvelimet ovat usein itsenäisiä (Baun, Kunze, yms. 2011, 3).

Pilvessä data voi siis sijaita missä tahansa, eikä käyttäjällä ole välttämättä tietoa missä hänen dataansa säilytetään. Työni kautta olen saanut havaita, että suomalaistenkin yritysten dataa kyllä säilytetään suomessa, mutta palvelun operointi voi tapahtua esimerkiksi intiassa. Palvelunostaja on siis riippuvainen palveluntuottajasta ja luottaa, että hänen palvelunsa tuotetaan vastuullisesti. Uutisista olemme voineet syksyn aikana lukea kuinka EU:n ja Yhdysvaltojen ns. Safe Harbour sopimus on todettu mitättömäksi. Käytännössä se määrittelee missä maissa on EU:n mukaan turvallista säilyttää yritysten ja kansalaisten tietoja digitaalisesti. Sopimus on hyvin tärkeä, sillä se määrittelee miten datan säilytys tulee tehdä turvallisesti. Kun sopimus Yhdysvaltojen kanssa mitätöity, voidaan olettaa datan säilytyksen vähentyvän Yhdysvalloissa EU maiden toimesta.

Yksi pilvipalveluita puoltava seikka on sen taloudellinen vaikutus. Niiden tiukka palveluorientoituminen, verkkostandardien ja internetin käyttöönotto integroituneena teknologiana sekä liiketoiminta-alustana tekevät pilvipalveluista hyvin soveltuvia monenlaisiin käyttötarkoituksiin. Nämä pitävät sisällään verkko-ohjelmistot ja modulaariset palvelut hajautuneissa liiketoimintaverkostoissa sekä prosessiketjuissa. (Baun, Kunze, yms. 2011, 3).

Monesti lainattu määritelmä pilvipalveluille syntyi Amerikassa National Institute of Tandards and Technology (NIST) toimesta. Määritelmä erittelee pilvipalveluille viisi olennaista ominaisuutta. Tärkeimmät ominaisuudet ovat:

1. Palvelut voidaan tarjota tarpeenmukaan ja ilman ihmisen toimintaan
2. Palvelut ovat saatavilla tietoverkon kautta reaaliaikaisesti standardoitujen toimintojen kautta
3. Resurssit ovat ryppäissä mahdollistaakseen paraalisen palveluiden jakamisen useille asiakkaille, samalla kun resursseja säädetään jokaisen käyttäjän vaatimuksia vastaavaksi
4. Resursseja jaetaan nopeasti ja hienojakoisesti jotta palveluita voidaan skaalata tarpeen mukaan. Käytäjälle resurssit vaikuttavat olevan rajattomat
5. Palvelut hyödyntävät kvantitatiivisia ja kvalitatiivisia menetelmiä, jotta käyttöön perustuva laskutus ja palvelun laadun validiointi olisivat mahdollisia (Baun, Kunze, yms. 2011, 3-4).

3 Syitä pilvipalveluiden yleistymiselle

Pilvi voi tarkoittaa montaa asiaa kuten sadepilveä, mutta tietotekniikassa puhutaan ”objektien kokoelmasta, jotka on yhdistetty ryhmäksi”. Nimenomaan ryhmäyttäminen tai resurssivarastojen luonti erottaa pilvipalvelut muista verkotetuista systeemeistä (Sosinsky 2011, 94).

Organisaatiot joutuvat taistelemaan asiakkaiden muuttuvien tarpeiden kanssa. Pilvipalvelut vastaavat tähän tarpeeseen. Mikäli palveluntarjoajan tietokoneresursseja ei jonakin aikana tarvita yhtäpaljon kuin jonakin toisena, pilvipalvelut voivat reagoida tähän muutokseen (Krutz, Russel 2010, 3).

Pilvipalvelut sallivat käyttäjien saada käyttöönsä resursseja tarpeenvaatiessa itsepalveluna ilman kanssakäymistä palveluntarjoajan kanssa. Käyttäjät voivat ajoittaa resurssien käyttöä omien tarpeidensa mukaan sen lisäksi, että itse toimittavat ja hallinnoivat näitä palveluita. Jotta asiakkaat suostuvat itsepalveluun on palvelun käyttöliittymän oltava asiakasystävällinen ja tarjota tehokkaat tavat hallinnoida näitä palveluita. Kanssakäymisen välttäminen tarjoaa kustannushyötyjä molemmille osapuolille (Krutz, Russel 2010, 9, 10).

Ollakseen kilpailukykyisiä yritysten omille datakeskuksille pitää yrityksellä olla käytössä nopeat tiedonsiirtolinkit pilvipalveluun. Yksi peruste pilvipalvelulle on madaltuneet kustannukset nopeille tiedonsiirtoverkoille. Nämä verkot antavat pääsyn suurempiin tietokoneresursseihin, jotka pystyvät ylläpitämään suurempaa käyttöastetta (Krutz, Russel 2010, 10).

Pilvipalvelulla on oltava suuri ja joustava resurssivarasto, jotta se voi pystyä vastaamaan asiakkaiden tarpeisiin, tuottaa suuruuden ekonomiaa ja vastata palvelutasovaatimuksiin. Ohjelmistot vaativat resursseja toimiakseen ja resurssit on tämän vuoksi allokoitava tehokkaasti, jotta paras mahdollinen suorituskyky voidaan saavuttaa. Nämä resurssit voivat sijaita missä tahansa, mutta ne voidaan osoittaa virtuaalisesti tarpeen mukaan. NIST:n mukaan asiakkaalla ei ole tarkkaa tietoa mistä saamansa resurssit tulevat, mutta voi saada tietoonsa yleisemmän sijainnin kuten mantereen, maan tai datakeskuksen (Krutz, Russel 2010, 10).

Pilvipalveluiden vetovoimaisuus on ainakin osittain siinä, että ne piilottavat it-teknologian monimutkaisuuden käyttäjiltä ja kehittäjiltä. Heidän ei tarvitse tietää yksityiskohtia palveluiden tuottamisesta, se on palveluntarjoajan tehtävä. Tässä kappaleessa käsitellään joitakin teknologioita joita tarvitaan pilvipalveluiden tuottamiseen. Näitä ovat esim. virtualisointi, palveluorientoitunut arkkitehtuuri (SOA) ja verkkopalvelut (Baun, Kunze, yms. 2011, 5).

Tietokoneresurssien virtualisointi on useimpien pilvipalvelutekniikoiden ytimessä. Virtualisointi sallii abstraktin eli loogisen näkymän fyysisiin resursseihin ja pitää sisällään

palvelimet, datan säilytyksen, tietoverkot ja ohjelmistot. Perusideana on laittaa fyysiset resurssit yhteen ja hallinnoida niitä kokonaisuutena. Yksittäiset palvelupyynnöt voidaan käsitellä näistä resursseista. On esimerkiksi mahdollista luoda dynaamisesti tietynlainen alusta tietynlaista tarkoitusta varten juuri sillä hetkellä kun sitä tarvitaan. Todellisen laitteen sijasta kuitenkin käytetään virtuaalista laitetta. (Baun, Kunze, yms. 2011, 5).

It-palveluiden tuottajalle virtualisoinnin käytöstä on monia etuja. Virtuaaliset laitteet pystyvät täyttämään resurssit tarpeet resurssivarannoistaan. Jos tarpeet kasvavat, on mahdollista viivästyttää tai jopa välttää kokonaan uuden kapasiteetin hankintaa. Virtuaalisia laitteita on myös helpompi hallinnoida. Resurssien hallintaa pystytään automatisoimaan ja niitä pystytään luomaan ja konfiguroimaan tarpeen vaatiessa. Erilaiset ohjelmistot voidaan voidaan konsolidoida käyttämään vähempiä fyysisiä komponentteja. Palvelin ja tallennustilan konsolidoinnin lisäksi on mahdollista luoda kokonaiskuvia järjestelmästä, datasta, tietokannoista, verkoista ja työpöydistä. Konsolidointi johtaa kasvaneeseen tehokkuuteeen ja siten rahallisiin säästöihin. (Baun, Kunze, yms. 2011, 5).

Suurien datakeskusten energiansaannin varmistaminen on yhä vaikeampaa ja palvelimien käyttöiän kuluttama sähkö on kalliimpaa kuin sen hankintahinta. Konsolidoinnin mahdollistama komponenttien vähentäminen auttaa virrankulutuksen laskemisessa, mikä tietää säästöjä yritykselle. Konsolidointi myös pienentää datakeskusten vaatimaa laitetilaa, mikä voi mahdollistaa datakeskuksen laajentamisen välttämisen. Virtuaalisia laitteita voidaan myös siirtää resurssivarannosta toiseen, mikä takaa paremman saatavuuden palveluille ja paremman palvelutason. Myös laitehuoltojen määrä saadaan laskemaan. (Baun, Kunze, yms. 2011, 5).

Virtualisointi ei johda pelkästään koon tuomaan etuun suurissa datakeskuksissa, vaan myös parempaan kustannustasoon asiakkaalle. Palvelupyynnöt voidaan suorittaa juuri oikeaan aikaan ilman viivytyksiä. Jos virtuaalinen laite törmää pullonkaulaan resurssien saatavuudessa, se voi pyytää niitä lisää. Palvelut ovat myös paremmin saatavilla ja niitä voidaan käyttää yötä-päivää ilman pysähdyksiä. Jos saataville tulee uutta teknologiaa, ohjelmistot voidaan siirtää päivitetylle virtuaalilaitteelle, vaikka ohjelmisto olisi käytössä. Virtuaalitaso eristää jokaisen virtuaalilaitteen toisistaan ja myös fyysisestä infrastruktuurista. Täten virtuaaliratkaisut voivat palvella useita asiakkaita kerralla ja hallinnointi on mahdollista delegoida helposti asiakkaalle. Asiakkaat voivat ostaa it-kapasiteettia itsepalveluportaalista (Baun, Kunze, yms. 2011, 5).

Virtualisoinnin huonona puolena voidaan pitää abstraktin tason operoinnin vaatimia resursseja. Modernit virtualisointitekniikat ovat kuitenkin niin kehittyneitä ettei tämä ole suuri ongelma. Nykyaikaisten laitteistojen moniydin suorittimet ja virtualisointiratkaisut ovat niin tehokkaita, että tämä suoritustasonlasku on vain pieni ongelma. Asiakkaan saamat säästöt ja palvelutason nousu ovat yleensä aina kannattavia syitä käyttää virtualisointia. Toinen ongelma on konsolidointi, yhä useampia laitteita pitää hallinnoida ja virtuaalisten

laitteiden lisäksi on myös fyysinen infrastruktuuri. Käyttämällä kehittyneitä hallinointityökaluja voidaan resursseja hallinnoida pienemmällä ihmismäärällä (Baun, Kunze, yms. 2011, 5).

3.1 Virtualisointi

Virtuaalinen laite on yleensä itsenäisen käyttöjärjestelmän kuva, johon on valmiiksi ladattu oikea konfiguraatio, ja joka on käyttövalmis. Tämän käyttöjärjestelmän tueksi tarvitaan hypervisor, joka esittää itsensä fyysisenä tietokonerautana vituaalikoneelle.

On olemassa erilaisia virtualisointeja, mitkä ovat ominaisia pilvipalveluille. Ensinnäkin käyttäjä voi pyytää pääsyä pilvipalveluun mistä tahansa sijainnista. Pilvipalvelulla on useita ohjelmistoinstansseja ja ohjaa palvelupyynnöt johonkin instanssiin riippuen olosuhteista. Tietokoneet voidaan partitioida eli osioida virtuaalikoneiksi, jolle kullekin osoitetaan oma työkuormansa. Vaihtoehtoisesti järjestelmät voidaan virtualisoida käyttämällä työkuorman balansoivaa ohjelmistoa. Dataa säilytetään läpi tallennuslaitteiden ja niitä replikoidaan useasti varmuuskopioinnin tähden. Mahdollistaakseen nämä ominaispiirteet resurssien täytyy olla todella hyvin konfiguroitavissa ja juostavia. (Sosinsky 2011, 94).

Virtualisointi tarkoittaa erilaisia konsepteja ja teknologioita, jotka eroavat toisistaan implementointoinnin, relevanttiuden, käytännöllisyyden ja käyttötiheyden perusteella. Käyttöjärjestelmän virtualisointi, kuten IBM LPAR, pilviympäristössä voi auttaa ratkaisemaan turvallisuus ja luottamuksellisuuteen liittyviä ongelmia, mitkä voivat haitata pilvipalveluiden hyväksyntää käyttöön (Baun, Kunze, yms. 2011, 7).

Tämän kaltaisessa virtualisoinnissa käyttöjärjestelmä on tärkeässä roolissa. Tässä konseptissa useat järjestelmä -ja suoritusympäristöt, jotka ovat täysin eristettyjä toisistaan, ajatetaan saman käyttöjärjestelmän kernelin päällä. Ulkoapäin katsottuna virtuaaliympäristöt näyttävät itsenäisiltä järjestelmiltä, mutta ne voivat havaita vain prosesseja, jotka kuuluvat samaan virtuaaliympäristöön (Baun, Kunze, yms. 2011, 7).

Tällä virtuaaliratkaisulla on hyvät ja huonot puolensa ja sitä käyttävät usein vain internetoperaattorit, koska se tarjoaa suurta tietoturvallisuutta ja vain pientä suorituskyvyn menettämistä. Huono puoli on sen jäykkyys: vaikka samaa käyttöjärjestelmää voidaan käyttää useaan kertaan itsenäisinä instansseina, mutta ei ole mahdollista käyttää useita eri käyttöjärjestelmiä samaan aikaan (Baun, Kunze, yms. 2011, 7).

Alustan virtualisointi sallii minkä tahansa käyttöjärjestelmän ja ohjelmistojen ajamisen virtuaalisessa ympäristössä. On olemassa kaksi eri mallia: täysi virtualisointi ja paraalinen virtualisointi. Molemmat ratkaisut implementoidaan virtuaalisen koneen monitoorin tai hypervisorin pohjalle. Hypervisor on minimalistinen meta-käyttöjärjestelmä, jota käytetään tietokoneen fyysisten resurssien jakamiseen. Hypervisoreita on kahta erilaista, tyyppi 1 ja

tyyppi 2. Tyypin 1 hypervisor toimii suoraan fyysisten resurssien päällä ja tyyppi 2 toimii perinteisen käyttöjärjestelmän alla. (Baun, Kunze, yms. 2011, 7).

Täydessä virtualisoinnissa simuloidaan koko tietokone virtuaalisine resursseineen, kuten prosessori, ram-muisti, ajurit, verkkoadapterit jne. sisältäen oman biossinsa. Koska virtualisoinnissa päästään käsiksi tärkeimpiin resursseihin, eli prosessoriin ja ram-muistiin, voidaan virtualisoidulta käyttöjärjestelmältä odottaa lähes yhtä nopeaa toimintaa, kuin jos virtualisointia ei olisikaan. Muut komponentit, kuten ajurit ja verkkoadapterit emuloidaan. Vaikka virtualisointi heikentää suorituskykyä, sallii se muokkaamattomien vieraiden käyttöjärjestelmien käyttämisen (Baun, Kunze, yms. 2011, 7).

Paraalinen virtualisointi ei tarjoa emuloituja komponentteja vieraille käyttöjärjestelmille, vaan pelkästään käyttöliittymän. Komponenttien käyttöä varten vierailevaa käyttöjärjestelmää pitää muokata, koska kaikki suorat pääsyt komponenteille pitää korvata vastaavalla hypervisorin rajapinnalla. Tätä toimintoa käytetään, jotta ohjelmat voivat kutsua toimintoja käyttöjärjestelmän kerneliltä (Baun, Kunze, yms. 2011, 7).

Kuten todettua, pilvipalvelut käyttävät resurssien yhdistämistä varastoiksi, jotka voidaan osoittaa käyttäjälle heidän tarpeensa mukaan. Näin ei ole kuitenkaan kaikkien pilviohjelmistojen kohdalla. Resurssien yhdistäminen ja niiden allokoiminen tarpeen mukaan muodostaa kuitenkin hyvin houkuttavia etuja, joten niiden käyttöönotto muodostuu prioriteetiksi. Ilman resurssien yhdistämistä on mahdotonta saavuttaa riittävää käyttöastetta, tarjota siedettäviä kustannuksia asiakkaalle ja reagoida proaktiivisesti tarpeisiin (Sosinsky 2011, 94).

3.2 Tallennustilan virtualisointi

Pilvijärjestelmät voivat tarjota myös dynaamisesti skaalautuvan tallennustilan palveluna. Tallennustilan virtualisointi tarjoaa monta etua. Perusideana on erottaa datan tallennus klassisista tiedostopalvelimista ja yhdistää tallenustila yhdeksi varastoksi. Ohjelmistot käyttävät näitä varastoja täyttääkseen dynaamisesti omat tallennustilan tarpeensa. Datansiirtoon käytetään erillistä SAN eli storage area network - ratkaisua tai local company network:ia (LAN). Pilvipalveluista tuleva data on yleensä web-objektien muodossa, joita voidaan hakea internetistä. Pilvipalveluiden dataa hallinnoidaan keskusjohtoisesti, mikä antaa paremmat mahdollisuudet hallinnoida dataa. Myös pääsyoikeuksia dataan voidaan skaalata helpommin. Näiden lisäksi keskujohtoinen hallinta auttaa alentamaan kustannuksia (Baun, Kunze, yms. 2011, 9).

Avain näiden varastojen synnyttämiseen on tuottaa abstrakti mekanismi, jotta looginen osoite voidaan yhdistää fyysiseen resurssiin. Tietokoneet käyttävät tätä tekniikkaa sijoittaakseen tiedostoja kovalevylle ja pilvipalveluverkot käyttävät tekniikoita luodakseen virtuaalisia palvelimia, virtuaalista tallennustilaa, virtuaaliverkkoja ja ehkä joskus jopa virtuaalisia

ohjelmia. Abstraktio mahdollistaa pilvipalveluiden avainhyödyn: jaetut ja kenen tahansa saatavilla olevan tiedon (Sosinsky 2011, 93).

Dataa voidaan myös jakaa eri kategorioihin. Tämä mahdollistaa automaattisen elinkaarihallinnoinnin implementoinnin. Korkeimmalle kategorialle varataan eniten kaistaa ja saatavuutta. Halvemmille kategorioille puolestaan vähemmän. Dataa voidaan siirtää kategoriasta toiseen vaikuttamatta palveluun. Virtualisoidussa ympäristössä suuriakin datamääriä voidaan varmuuskopioida ilman erityisiä varmuuskopiointikatkoja (Baun, Kunze, yms. 2011, 9).

4 Pilvipalveluiden taloudelliset edut

Pilvipalveluiden käytöllä on mahdollisuus päästä merkittäviin taloudellisiin säästöihin ja kustannuksia on mahdollista myös optimoida. Niiden avulla voidaan laskea kustannuksia välttämällä kustannusten syntyä ja maksaa vain käytöstä. Lsiäksi tietokoneiden resurssit ovat tehokkaammassa käytössä virtualisoinnin kautta ja kaiken lisäksi omalle it-osastolle voidaan näiden saavutusten takia palkata vähemmän ihmisiä töihin. Kumuloituneet säästöt voivat olla merkittäviä erityisesti yrityksille, jotka välttävät investointeja datakeskuksiin sekä muihin it-kustannuksiin. Pilvipalvelut auttavat myös yritystoimintaa olemaan ketterämpiä ja toimittamaan palvelunsa nopeammin markkinoille (Marks, Lozano 2010, 78, 79).

Virtualisoinnin yksi hyvä puoli on, että se nostaa palvelimien käyttöastetta merkittävästi. Sen avulla käytöastetta on mahdollista nostaa tavallisesta 10%:sta kymmenillä prosenteilla jopa 65% asti tai joskus jopa vielä korkeammaksi. Tämä käyttöasteen nosto voidaan saada aikaan myös tallennusratkaisujen virtualisoinnille. Tällainen nousu käyttöasteessa vaikuttaa laskevasti myös kustannuksiin, mukaan lukien käyttökustannukset, huoltokustannukset ja henkilökunnasta syntyvät kustannukset. Pilvipalvelut antavatkin mahdollisuuden ulkoistaa koko oman it-infrastruktuurin. Näin tehdessään yritys voi antaa oman it-henkilökunnan keskittyä strategisempiin ja innovatiivisempiin vaatimuksiin. Tällainen toiminta on parempaa henkilökunnan osaamisen ja taitojen käyttöä, mikä antaa paremman vastineen heihin sijoitetulle pääomalle (Marks, Lozano 2010, 79).

Vain käytöstä maksaminen on pilvipalveluiden avain ominaisuus. Tällöin tietokoneresursseja, mukaan lukien datan tallenuksen ja ohjelmistoresurssit, käytetään vain tarvittaessa ja asiakas maksaa vain siitä minkä verran näitä resursseja on käyttänyt. Mikäli asiakas lopettaa tai ei tarvitse resursseja, ne otetaan takaisin ja ovat jonkin toisen käytettävissä. Näin resurssit eivät ole toimettomina synnyttäen silti kustannuksia riippumatta käytetäänkö niitä vai ei. Jos asiakas haluaa lisäresursseja, on niitä myös nopeampaa hankkia pilvipalveluna. Resurssien nopea saatavuus on yksi suuri syy miksi yritykset siirtyvät pilvipalveluihin. Normaalisti lisäresurssien hankinta on niin työlästä, että kaikki ratkaisut, jotka auttavat tähän ongelmaan otetaan vastaan (Marks, Lozano 2010, 80).

Pilvipalvelut auttavat yrityksiä pääsemään käsiksi pilvipohjaisiin resursseihin, jotka ovat jo asennettu, konfiguroitu ja valmiita käytettäviksi vain luottokorttia käyttämällä. Pilvipalvelut siis helpottavat palveluiden ostamista. Ostoprosessien helpottaminen on myös yksi suuri syy pilveen siirtymisessä. Hitaat ostoprosessit voivat haitata projektien etenemistä. Pilvipalveluiden avulla voidaan käyttää standardia ostoprosessia, jolloin ajankäyttö prosessin läpikäymiseen lyhentyy (Marks, Lozano 2010, 81).

Mahdollisuus päästä käsiksi ryvästettyihin resursseihin maksamalla vain käytöstä tarjoaa monia tekijöitä, jotka kokonaan muuttavat informaatioteknologian infrastruktuurin ekonomian ja sallivat uudenlaisia käyttö -ja liiketoiminta malleja käyttäjän ohjelmistoille. Pilvipalvelu on infrastruktuuri, joka voidaan osioida ja provisioida. Resurssit on ryvästetty ja virtualisoitu. Suurien datakeskusten rakentaminen, jotka käyttävät tavallisia tietokonekomponentteja, ovat mahdollistaneet pilvipalveluiden suosion kasvun. Näillä keskuksilla on pääsy halvempaan sähköön, nopeisiin verkkoyteyksiin sekä halpoihin komponentteihin ja ohjelmistoihin. Nämä yhdessä muodostavat suuruuden ekonomian, mikä sallii palveluntarjoajien saada sijoituksilleen tuottoa (Sosinsky 2011, 24, 25).

Ryvästettyjen resurssien virtualisointi optimoi nämä investoinnit ja sallii palveluntarjoajan tarjota nämä ekonomiset edut asiakkailleen. Ryvästäminen myös sumentaa erot pienen ja suuren palvelun välillä, koska koko riippuu ainoastaan kysynnästä. On monia syitä miksi yritykset suuntautuvat pilvipalveluidentarjoajiksi. Yksi niistä taloudellinen voitto, suuruuden ekonomia mahdollistaa pilvipalveluiden olevan taloudellisesti kannattavaa. Myöskin infrastruktuuri on valmiina, eikä sitä ole vielä käytetty täydessä mitassaan. Pilvipalvelut myöskin lisäävät yrityksen tuotevalikoimaa ja puolustaa heidän markkina-asemaansa. Hyvin markkinoitu pilvipalvelualusta voi lisätä asiakkaan suhdetta yritykseen tarjoamalla lisäpalveluita. Tämä on esimerkiksi paikkaansa pitävää IBM:n kohdalla heidän tarjotessaan monia pilvipalveluitaan. Pilvipalvelut voivat tuoda yrityksen markkinoille ennen suurta kilpailijaa. Pilvipalveluidentarjoaja voi myös kohota tärkeäksi tekijäksi itsenäisten ohjelmistojen tarjoajana. (Sosinsky 2011, 25, 26).

Iso osa pilvipalveluiden arvosta ja vetoavuudesta on sen kyky muuttaa hankintakustannukset käyttökustannuksiksi käyttämällä käyttöön perustuvaa hinnoittelua, joka on joustava ja voidaan mitoittaa oikein. Oikeiden assettien muuttaminen virtuaalisiksi tarjoaa suojauksen liian suurta tai pientä infrastruktuuria vastaan. Pähkinänkuoressa: kustannusten muunto käyttökustannuksiksi sallii riskin siirtämisen palveluntarjoajalle (Sosinsky 2011, 35).

Pilvipalveluiden muita etuja ovat vapaus palvelimien ja ohjelmistojen päivittämiseltä. Uudet ja palvelut teknologiat provisioidaan automaattisesti. Lisäksi lisäresursseja saadaa tarpeenvaatiessa ja organisaatio pystyy keskittymään innovaatioihin huoltotoimenpiteiden sijaan. Pilvipalvelut tarjoavat suuret resurssit datan tallentamiseen, jotka ovat normaalisti organisaation sisällä lokaalisti. Näitä resursseja voidaan tarpeenvaatiessa joko vähentää tai kasvattaa ja samalla myös hinta asiakkaalle noudattelee tarpeen muutosta. Myöskin datan

turvaaminen ja monitorointi on helpompaa keskitetyssä järjestelmässä. (Krutz, Russel 2010, 57, 58).

Kuten aina, hyötyjen kanssa tulee myös haittapuolia. Pilvipalveluissa riskinä on säilyttää suuria määriä sensitiivistä tietoa suuressa keskitetyssä ympäristössä. Tällainen keskitetty järjestelmä voi kiinnostaa tunkeutujia tai rikollisjärjestöjä. Vasta-argumenttina voidaan käyttää, että turvaamistoimenpiteet voidaan paremmin keskitetyssä järjestelmässä kuin jaetussa, kunhan nämä toimenpiteet tehdään ammattitaidolla (Krutz, Russel 2010, 10).

Pilvipalvelut myös lyhentävät aikaa joka kuluu palvelun tuotantoon tulemiseen. Pilvipalvelut tarjoavat tapoja tuoda suuria laskenta -ja tallennusresursseja lyhyessä ajassa ilman mittavia alkuinvestointeja fyysisiin resursseihin, ohjelmistoihin tai henkilökuntaan (Krutz, Russel 2010, 58).

Palvelutasosopimukset (SLA) ovat sopimuksia joissa määritellään palvelun minimitaso asiakkaalle. Se on pilvipaluissa ainoa käytännön sopimus, joka määrittää palveluntarjoajan vastuun rajat palvelun toimivuudesta. Täten se turvaa asiakasta sopimusrikkomukselta (Viinikka 2013, 47.) Sopimukseen voidaan päästä joko alekirjoittamalla laillinen ja pitävä sopimus tai tai epävirallisesti yrityksen eri osastojen välillä. SLA viittaa yhteiseen sopimukseen jossa kunnioitetaan turvallisuutta, prioriteetteja, vastuita, takuita ja laskutuskäytäntöjä. Lisäksi SLA määrittelee erilaisia mittareita kuten: saatavuus ja vasteajat. Palvelutasosopimuksille on tyypillistä, että niitä muodostetaan palvelunkäyttäjän näkökulmasta. Tuottaja voi erottua edukseen tuottamalla erityisen hyvää palvelua tai erityisen innovatiivisella tavalla. Aikaisemmin sopimukset neuvoteltiin palveluntarjoajan ja heidän asiakkaiden välillä, nykyään sopimukset on standardoitu kunnes asiakkaasta tulee suurasiakas. Tähän kehitykseen on päästy suurien pilvipalvelutarjoajien ilmestyttyä markkinoille (Sosinsky 2011, 39).

Pilvipalveluiden palvelutasosopimukset kontrolloivat resurssien allokointia ja resurssien dynaamista käyttöä. Palvelutasojen hallintaan on kaksi tärkeää vaihetta: palvelutasosta sopiminen ja palvelun monitorointi sitä käytettäessä. Nykyisillä pilvipalveluilla palvelutasosta sopiminen ja sen valvominen on mahdollista vain perustasolla ja palvelut tuotetaan ”parhaan yrityksen” perusteella (Baun, Kunze, yms. 2011, 40).

5 Pilvipalveuihin kohdistuvat uhkatekijät

Tähänasti on käsitelty pilvipalveluiden yleisiä periaatteita ja teknisiä ratkaisuja sekä taloudellisia syitä siirtyä pilvipalveluiden käyttöön. Pilvipalveluista on hyötyä paitsi asiakkaalle niin myös palveluntarjoajalle laskevina kustannuksina. Toinen osa tätä työtä on hankkia tietoa pilvipalveluiden tietoturvallisuudesta, kuinka niiden turvallisuus voidaan taata, ovatko ne yleensäkään tietoturvallisia ratkaisuita säilyttää dataa ja minkälaisia uhkia niitä vastaan kohdistuu.

On julkisesti tiedossa, että verkkopalvelut kuten Facebook ja Google keräävät käyttäjistään valtavia määriä tietoa. Tätä tietoa ne myyvät mainostajille ansaitakseen liiketoiminnallaan taloudellista voittoa. On myös selvää, että rikolliset ovat kiinnostuneita myös tästä tiedosta, sillä sitä myymällä voi saada rahaa. Täten on erittäin tärkeää, että tietoa suojataan asianmukaisesti, mutta myös käyttäjien kannattaa varmasti miettiä mitä tietoa itsestään palveluihin tallentaa.

Viimeaikoina olemme suomessakin saaneet lukea mediasta, että poliisi ja puolustusvoimat ovat kiinnostuneita pääsemään käsiksi kansalaisten vekkoliikenteeseen. Tätä puolustetaan rikollisuuden -ja terrorismintorjunnalla. Tietoliikenteen kunnollinen suojaaminen on nykyisenlaisessa verkottuneessa ja tietokoneiden ohjaamassa maailmassa erityisen tärkeää. Mediasta on voinut lukea myös F-securen toimitusjohtajan puhuneen tietoturvayhtiöiden ennen turvanneen tietokoneita, mutta nykyään yhteiskuntaa. Hän on oikeassa, sillä olen oman työni kautta saanut todistaa kuinka tietokoneet ylläpitävät esimerkiksi suomalaisia pankkipalveluita. Jokainen voi kuvitella mitä yhteiskunnalle tapahtuu jos pankki -tai muita kriittisiä yhteiskunnan palveluita onnistuttaisiin tuomaan alas rikollisuuden tai terrorismin avulla.

Monet kuitenkin pelkäävät valvonnan lisäämisen johtavan jopa Orwellilaiseen pakkoyhteiskuntaan. Valvonnan lisäämisen hyödyistä ja haitoista onkin hyvä keskustella avoimesti. Jokainen voi itse miettiä mitä itsestään internetissä julkaisee ja kuinka avoimesti elämästään internetissä kertoo. On mielestäni kuitenkin ilmeistä ettei tavallisen ihmisen normaaliin elämään kuuluvista asioista ole kiinnostuneita kuin julkaisija itse ja ihmiset, jotka hänen julkaisujaan lukee. Vastapainona on kuitenkin myös mahdollisuus havaita vakavia rikoksia etukäteen ja siten lisätä kansalaisten turvallisuutta. Tässä työssä ei ole kuitenkaan tarkoitus selvittää kuinka yksittäisen ihmisen tulisi toimia internetissä, vaan kyse on pilvipalveluiden turvaamisesta yritysten näkökulmasta. Pilvipalveluita uhkaavat monet tekijät, joita käsitellään seuraavaksi.

Suurin haaste pilvipalveluissa on niiden turvallisuus. Voidaan kysyä: Onko meillä mitään takeita ettei dataamme ole pääsyä hyväksymättömällä käyttäjällä? Koska sensitiivistä dataa käsitellään yrityksen ulkopuolella, tuo se mukanaan riskejä. Ulkopuoliset palvelut ohittavat fyysiset, loogiset ja ihmisten muodostamat turvakontrollit. Tämän takia olisi hyödyllistä kerätä dataa käsittelevistä ihmisistä mahdollisimman paljon dataa ja kysyä palveluntarjoajilta tarkkaa tietoa kuinka he palkkaavat ja valvovat dataa käsitteleviä adminstraattoreita sekä heitä valvovia kontrolleja (Mahdavi, Nazem 2009, 1115).

Loppujen lopuksi asiakkaat ovat vastuussa datansa turvallisuudesta ja eheydestä, vaikka sitä säilyttäisikin jokin ulkopuolinen taho. Palveluntarjoajiin kohdistuu perinteisesti ulkopuolisten suorittamia audit-tarkastuksia sekä sertifiointeja. Jos pilvipalveluntarjoaja kieltäytyy näistä, on viisasta olla käyttämättä sellaista tarjoajaa (Mahdavi, Nazem 2009, 1115).

Kuten todettua pilvipalveluissa säilytettävän datan fyysistä olinpaikkaa ei välttämättä ole käyttäjän tiedossa. Palvelunostajan voi olla kuitenkin mahdollista pyytää palveluntuottajaa säilyttämään dataa jollakin tietyllä alueella sekä noudattamaan sen alueen yksityisyydensuojasäännöksiä. Koska dataa säilytetään jaetussa ympäristössä, on tärkeää huolehtia datan salakirjoittamisesta. Lisäksi on tärkeää selvittää miten palveluntuottaja suojaa dataa sen ollessa levossa. Tuottajalta onkin hyvä vaatia todisteita salakirjoittamisen tuottamisesta ammattilaisten toimesta. Salakirjoittaminen voi myös vahingon sattuessa tehdä datasta käyttökelvotonta. Jopa normaali salakirjoitus voi uhata datan saatavuutta (Mahdavi, Nazem 2009, 1115).

Mikäli dataa ei ole asianmukaisesti salakirjoitettu, on se helposti kaapattavissa, kun sitä liikutetaan verkossa. On hyvä muistaa, että kovalevyt joilla dataa säilytetään on tuhottava, kun ne poistetaan käytöstä. Vaikka kovalevy olisi poistettu käytöstä pitää se fyysisesti tuhota tai ohjelmallisesti ylikirjoittaa riittävän useasti, jotta sillä oleva data on varmasti käyttökelvotonta kenenkään luettavaksi. Tätä olen saanut todistaa useasti omassa työssäni, kun asiakas kieltäytyy antamasta rikkoutunutta kovalevyä takaisin saadessaan uuden. Samaa tarkkuutta tietoturvallisuuden osalta käytetään myös palvelimien osalta. Tiedän tapauksen, jossa asiakkaalta on poistunut käytöstä palvelimia ja ne pitäisi hakea pois, mutta asiakas kieltäytyy kunnes palvelimien kiintolevyt on putsattu tietoturvallisesti. Eräässä tapauksessa asiakas vaati dokumentointia kiintolevyjen tuhoamisprosessista ja takuita kiintolevyjen tyhjentämisestä.

Joskus tietotekniikassa tapahtuu ikäviä yllätyksiä. Tällaisia yllätyksiä voi tapahtua esimerkiksi normaalien huoltotoimenpiteiden yhteydessä. Tällöin on erittäin tärkeää, että palveluntarjoajalla on hätätilanteita varten suunnitelma datan sekä palvelun palauttamisesta. Mikä tahansa palvelu, joka ei tallenna dataa ja ohjelmistoja useisiin fyysisiin paikkoihin on haavoittuvainen täydelle käyttökatkolle. Asiakkaan on tärkeää kysyä onko hänen tarjoajallaan mahdollisuus tehdä täydellinen datanpalautus ja kuinka kauan se kestäisi (Mahdavi, Nazem 2009, 1115).

Epäasiallisen tai jopa rikollisen toiminnan tutkiminen voi olla haastavaa pilviympäristössä. Pilvipalvelut ovat hankalia tutkittavia, koska dataa voidaan tallentaa useassa paikassa ja se voi olla levittäytyä aina uusiin isäntätietokoneisiin ja datakeskuksiin. Tämän takia asiakkaan tulisi pyytää todisteita, että palveluntarjoaja on aikaisemmin tukenut selvityspyyntöjä. Selvityspyyntöjen tukeminen tulisi myös mainita yritysten välisessä sopimuksessa (Mahdavi, Nazem 2009, 1115).

Joskus yritykset ostavat toisiaan tai yhdistyvät. Tämän takia on tärkeää varmistua siitä, että datan saatavuus ei vaarannu vaikka tällainen tapahtuma tulisikin todellisuudeksi. On myös tärkeää kysyä kuinka datan saa takaisin, jos näin tapahtuisi ja olisiko se sellaisessa muodossa jonka pystyy siirtämään toiseen säilytyspaikkaan (Mahdavi, Nazem 2009, 1115, 1116).

Pilvipalvelut ovat riippuvaisia verkkoyhteyksistä ja verkon toimimattomuus on suuri uhka. Mikäli verkko menee epäkuntoon tai ei ole käytettävissä mistä tahansa syystä, on lopputuloksena katastrofi mikä ei eroa onnistuneesta palvelunestohyökkäyksestä. Verkkoyhteyden tulee olla tarpeeksi nopea ja kaistaltaan riittävän suuri, jotta verkko on aina käytettävissä (Vic W 2011, 56).

Palvelun ostajan on pystyttävä olemaan varma, että heidän ostamansa palvelu jatkuu vaikka palveluntarjoajan tuotantojärjestelmässä tapahtuisi jokin katastrofi. Palveluntarjojan on huolehdittava omista varmistuksistaan ja varauduttuva riittävillä toimenpiteillä kaikenlaisiin mahdollisiin tilanteisiin niin ettei palvelut ole uhattuina. Asiakkaita tulee myös informoida, jos palvelut ovat uhattuina. Palveluntarjoajat eivät aina paljasta asiakkailleen sisäisiä tapojaan toimia palveluiden turvaamiseksi ja silloin asiakkaan on luotettava heidän väitteisiinsä turvallisuudesta. Tästä huolimatta tulisi vaatia jonkinlaista läpinäkyvyyttä ongelmatilanteiden hallintaan (Vic W 2011, 56).

Virtualisointi tuottaa myös uhkan pilvipalvelulle tuomalla uusia käyttöjärjestelmiä yläpidettäviksi. Virtuaalikoneiden mukana tulevat uudet käyttöjärjestelmät ovat jo itsessään uhkia ja siksi niitä pitää jatkuvasti päivittää ja ylläpitää. Tyypilliset verkkopohjaiset murtautumisen tunnistusjärjestelmät eivät toimi hyvin virtuaalisten palvelimien kanssa. Tämän takia on käytettävä kehittyneempiä tapoja virtuaalisten palvelimien välisen verkkoliikenteen tarkkailuun (Vic W 2011, 58).

Virtualisoinnin myötä tulee ilmeiseksi, että tavat joilla hallinnointiin perinteisiä fyysisiä palvelimia eivät toimi virtuaaliympäristössä. Tyypillinen tapa hallinnoida fyysisiä palvelimia ei sisällä niiden automaattista käyttöönottoa ellei niiden määrä ole huomattava. Fyysisten palvelimien kohdalla käyttöönotossa vaaditaan pääkäyttäjältä aina tietyt toimenpiteet. Tilanne on toinen virtuaalisessa ympäristössä. Silloin on kyseessä korkeasti automatisoitu prosessi (Vic W 2011, 59).

virtualisointi tuo monia turvallisuuskysymyksiä joita on hyvä pohtia. Ensinnäkin: jos hypervisor on altis turvallisuusuhille siitä tulee pääasiallinen uhkien kohde. Pilvipalveluiden laajuudella sillä olisi laajoja vaikutuksia, jos uhkaa ei pystytä minimoimaan eristämällä se verkosta, tai jos uhkaa ei havaita turvallisuutta muuten tarkkailemalla (Vic W 2011, 59).

Toinen virtualisoinnin tuottama uhka liittyy resurssien, jotka liittyvät virtuaalisiin palvelimiin, kuten tallennustilan allokointiin. Jos virtuaalipalvelimen käytön aikana dataa kirjoitetaan fyysiselle medialle tai muistille, eikä sitä tyhjennetä ennen kuin data allokoidaan seuraavalle virtuaalilaitteelle, voi kyseessä olla tiedon leviäminen ulkopuolisille. Sensitiivistä dataa tulisi aina käsitellä huolellisesti. Kolmas uhka on mahdolliset verkkohyökkäykset virtuaalikoneiden välillä. Jos jokaisen virtuaalikoneen verkkoliikennettä ei monitoroida, ei voida olla myöskään varmoja, että verkkoliikenne ei ole mahdollista virtuaalikoneiden välillä (Vic W 2011, 61).

Virtualisointi monimutkaistaa infrastruktuurin hallinointia, mutta pilvipalveluiden ollessa kyseessä sen täytyy olla automaattista. Virtualisoinnin takia suunnittelu ja hallinnointi tulee suorittaa paremmin kuin perinteisessä ympäristössä. Virtuaalisen pilviympäistön automatisoinnilla saavutetaan kuitenkin huomattavia etuja, myöskin parempaa turvallisuutta (Vic W 2011, 62).

5.1 Uhat yksityisyydelle

Tässä työssä on aikaisemmin jo sivuttu pilvipalveluiden tuottamaa uhkaa ihmisten yksityisyydelle. Nämä uhat ovat uhkia myös yrityksille. Yksikään yritys ei voi vähätellä maineen ja uskottavuuden menetyksen kustannuksia omalle liiketoiminnalleen. Mikäli yritys käsittelee yksityisyydensuojan piiriin kuuluvaa tietoa, on sen kiinnitettävä aivan erityistä huomiota tämän tiedon suojelemiseen. Kaikenlaiset internetsivujen ylläpitäjät hallinnoivat käyttäjiensä yksilöintiin soveltuvaa tietoa. Tällaista tietoa on esimerkiksi: nimet, osoitteet, puhelinnumerot. Lisäksi sivujen ylläpitäjät tallentavat käyttäjien salasanoja sekä käyttäjätunnuksia. Mikäli sivusto tarjoaa maksullista sisältöä on heillä pääsy käyttäjiensä luottokorttitietoihin. Nämä tiedot on ehdottomasti pidettävä salassa.

Yksi virhe, minkä organisaatiot usein tekevät, on antaa vastuu yksityisyyden tuomista riskeistä it-osastolle eikä liiketoimintayksikölle, joka omistaa datan. Tietojenkäsittelyjärjestelmät omaavat kehykset, joissa on määriteltynä standardoidut prosessit, jotka sopivat pilvipalveluihin ja mahdollisiin yksityisyydensuojan murtoihin (Krutz R, Russel V 2010, 126, 127).

Jokainen organisaatio, joka tallentaa, prosessoi tai välittää luottokorttitietoja eteenpäin, on velvollinen nuodattamaan luottokorttiyritysten välistä turvallisuusstandardia (PCI DSS) riippumatta luottokorttitapahtumien määrästä vuodessa. Jos yritys ei täytä standardin vaatimuksia, odotetaan siltä suunnitelmaa aukkojen paikkaamiseen. Jos vaatimuksiin ei suostuta, on luvassa sakkoja yrittäjälle, vaikka tietoja prosessoisi ja säilyttäisi kolmas osapuoli. Yritys joutuu todistamaan standardin noudattamisen. Isommat yritykset auditoidaan vuosittain ja pienemmät yritykset toimittavat vaadittavat dokumentit, joissa todistavat täyttävänsä standardin organisaatiot kehittävät ja julkaisevat yksityisyydensuojan ohjesääntöjä, joissa kuvaavat tapaansa käsitellä henkilökohtaista tietoa. Nämä ohjesäännöt on tavallisesti saatavilla yritysten internetsivuilta. (Krutz R, Russel V 2010, 129, 131).

Euroopan unionin parlamentin ja komissio nimittää erityisen eurooppalaisen datan suojaamiseen erikoistuneen valvojan (EDPS). EDPS julkaisee suosituksia euroopan yhteisölle. Se voi myös yrittää vaikuttaa EU-lakien valmisteluun siltä osin, kun ne koskevat henkilökohtaisen tiedon käsittelyä. EDPS osallistuu poliittiseen keskusteluun ja yrittää varmistaa, että pilvipalveluita tarjoavat yritykset toteuttavat EU-lainsäädäntöä datan suojaamiseksi. Se aikoo myös julkaista ohjeet varmistaakseen EU-instituutoiden, jotka

käyttävät pilvipalveluita, tekevän niin EU:n datan suojaamiseen tarkoitetun lain mukaan (European Data Protection Supervisor).

Monissa yksinkertaisissa asioissa vastuut henkilökohtaisen tiedon osalta on helppo määritellä. Asiakas eli datan kontrolloija, määrittelee miksi ja kuinka henkilökohtaista tietoa tulee käsitellä. Yritys puolestaan toimii vain asiakkaan ohjeiden mukaan. Pilvipalveluiden osalta asia ei ole kuitenkaan näin yksinkertainen, koska yritys tekee monia päätöksiä asiakkaansa puolesta. Näihin päätöksiin kuuluvat esimerkiksi: missä tietoa säilytetään, alihankkijoiden mahdollinen käyttäminen ja turvallisuus (European Data Protection Supervisor).

Pilvipalveluissa henkilökohtaisen tiedon kontrolli on yleensä jaettu asiakkaan ja palveluntarjoajan välillä. Tämä on merkittävä ero tavalliseen järjestelmään missä asiakas oli kontrolloija ja yritys prosessoija. Jos velvollisuuksien ja vastuiden jako ei heijastele eri osapuolien rooleja pilvipalveluiden tarjoamisessa, on suuri vaara että kukaan ei ota todellista vastuuta datan suojaamiseksi kuten laissa on määritelty (European Data Protection Supervisor).

Pilvipalveluiden ostajien tulisi olla selvillä sopimuksista, joita tekevät. Heidän tulisi ymmärtää, kuinka heidän tietojaan suojataan pilvessä. Palveluntarjoajien pitäisi myös selvittää avoimesti, kuinka he aikovat dataa suojata (European Data Protection Supervisor).

Henkilökohtainen tieto menee monesti yli rajojen ja sitä säilytetään ympäri maailman. EU:n ulkopuolella on erilaiset lainsäädännöt henkilökohtaisen tiedon suojaamiseksi eivätkä ne välttämättä anna samanlaista suojaa. Tämä luo uhan, että tietoon voi päästä käsiksi rajoitteitta ja jopa uhan väärinkäytöksille ilman käyttäjän kykyä harjoittaa oikeuksiaan suojella tietojaan, kuten he pystyisivät tekemään EU:n lainsäädännön alla (European Data Protection Supervisor).

Tämän takia yritysten, jotka säilövät asiakkaidensa tietoja EU:n ulkopuolella, täytyy sopimusten tai sitovien yrityssääntöjen avulla taata asiakkaiden tietojen säilytys tavalla, joka saavuttaa saman datan suojaamisen tason kuin se olisi EU:n alueella. Viranomaiset saattavat kysellä palveluntajoajilta, jotka ovat heidän toimialueellaan, pääsyä tietoihin, jotka on tallennettu pilveen. Palveluntarjoaja voi silloin kohdata ristiriitaisia laillisia vaatimuksia. Ideaalissa tilanteessa asiakkaita informoitaisiin sellaisesta pyynnöstä. EDPS suosittelee, että sellaista tietoa annettaisiin viranomaisille vain tiettyjen prosessien mukaisesti, jotka on määriteltynä kansainvälisillä sopimuksilla (European Data Protection Supervisor).

Euroopan unionin lait yksityisyyden suojaamiseksi suojaavat yksityisyyttä kuten lait Yhdysvalloissa. Tämäntakia yksityisten tietojen siirtäminen EU:sta Yhdysvaltoihin on kiellettyä, ellei samantasoisia säädöksiä noudateta. EU:n säädösten mukaan dataa tulee kerätä vain lainmukaisesti eikä tietoja saa antaa kolmannelle osapuolelle, jollei siihen ole laillista lupaa tai lupaa henkilöltä itseltään. Tiedot tulisi myös pitää paikkaansapitävinä sekä ajantasalla. Yksilöillä on lisäksi lupa korjata virheet heistä kerätyissä tiedoissa ja saada

raportti heistä kerätyistä tiedoista. Tietoa tulisi myös käyttää vain siinä tarkoituksessa, johon se on tarkoitettu ja vain järkevänpituisen ajan verran. Tiedon kuljettaminen paikkaan, jossa vastaavankaltaista tietoturvallisuutte ei voida taata on kiellettyä (Krutz R, Russel V 2010, 140, 141).

5.2 Uhat infrastruktuurille, datalle ja pääsynhallinnalle

Kuten aina tietoturvallisuuden turvaamisessa, myös pilipalveluiden turvaamisessa on kyse datan eheyden, saatavuuden ja luottamuksellisuuden varmistamisesta. Mikä tahansa tapahtuma mikä uhkaa näitä datan turvallisuuden ominaisuuksia voidaan luokitella uhkaksi. Mitään järjestelmää on mahdotonta suunnitella täysin turvalliseksi, sellaiseksi ettei mikään uhka pystyisi murtautumaan käytettävään tietokonejärjestelmään. Vaikka järjestelmä olisi suunniteltu teknisesti kuinka turvalliseksi tahansa on jäljellä aina ihminen, joka onkin monesti suurin uhka tietoturvallisuudelle.

Kun joku haluaa murtautua järjestelmään, etsii hän tuosta järjestelmästä haavoittuvuuksia. Krutz ja Russel määrittelevät haavoittuvuuden olevan järjestelmän heikkous, jota uhka voi hyväksikäyttää. Heidän mukaansa vähentämällä haavoittuvuuksia järjestelmässä voidaan vähentää riskejä ja uhkien tuottamaa vaikutusta järjestelmälle.

Pilvipalvelut ja normaalit tietokonejärjestelmät ovat alttiita samankaltaisille uhkille. Yksi näistä on salakuuntelu ja tiedustelu. Dataa voidaan kerätä, analysoida, käyttäjien näppäilyjä voidaan vakoilla, ja jopa roskakoreista voidaan yrittää kerätä tietoa. Salakuuntelu onkin pääasiallinen syy datan luottamuksellisuuden pettämiselle. Dataa voidaan myös manipuloida ja tehdä valheellisia datansiirtoja, jotta tieto ei olisi enää eheää. Dataa voidaan myös varastaa taloudellisen hyödyn saamiseksi. Esimerkiksi yrityssalaisuudet, fyysiset tietokoneosat ja ohjelmistot ovat varkaiden kohteina. Palveluita voidaan myös yrittää saboitoida ja häiritä esimerkiksi palvelunestohyökkäyksillä. Kaiken lisäksi hyökkäyksiä voidaa tehtailla organisaation ulkopuolelta. Tähän hyökkäystapaan soveltuu esimerksiksi haitalliset ohjelmat kuten haitallinen koodi ja viukset (Krutz R, Russel V 2010, 142).

Julkiset ja yksityiset pilvet eroavat tietoturvallisuudeltaan toisistaan. Ykstyinen pilvi ei eroa tietoturvallisuudeltaan perinteisestä tietokoneinfrastruktuurista, koska ne ovat keskenään hyvin samankaltaiset. Täten samat tavat joilla turvataan perinteisiä tietojärjestelmiä soveltuvat myös yksityiseen pilvipalveluun. Asia on kuitenkin toinen puhuttaessa julkisesta pilvestä. Julkisen pilven käyttäjät joutuvat miettimään uudelleen omaa tietoarkkitehtuuriaan ja prosessejaan. Lisäksi tulisi huomioida oman ja palveluntarjoajan verkkojen yhteensopivuus. Kaikissa tapauksissa turvallisen pilvearkkitehtuurin tulee pienentää riskiä tiedon eheydelle, saatavuudelle ja luottamuksellisuudelle ja taata riittävä pääsynhallinta, johon kuuluvat autentikointi, autorisointi ja auditointi (Krutz R, Russel V 2010, 129, 142).

Pilvipalveluissa tulee pääsynhallintaa kiinnittää huomiota. Sitä tulee ajatella sen kannalta kuinka arvokasta tietoa ollaan suojaamassa. Tiedon arvo voidaan määrittää kvalitatiivisilla ja kvantitatiivisilla metodeilla. Tiedon arvoa määritettäessä tulee miettiä sen arvoa organisaatiolle itselleen ja sen kilpailijoille, jos tieto paljastuu. Kunnollinen pääsynvalvonta takaa täyden saatavuuden datalle. Saatavuus takaa, että autorisoiduilla käyttäjillä on aina pääsy dataan (Krutz R, Russel V 2010, 145).

Pääsynhallinnan tulee tarjota suojaa autorisoimattomalta, odottamattomalta ja tarkoituksettomalta tiedon muokkaukselta. Suojaamisen tulisi kuitenkin säilyttää tiedon sisäinen ja ulkoinen johdonmukaisuus. Myös datan luottamuksellisuus on säilytettävä ja data tulisi olla saatavilla ajallaan. Pääsynhallintaan liittyy myös vastuullisuus – käyttäjät ovat vastuussa teoistaan. Vastuullisuus mahdollistaa järjestelmän toimintojen jäljittämisen tiettyyn yksilöön. Auditointi tukee vastuullisuutta sillä se tutkii lokitiedostot sekä järjestelmästä että verkosta. Yksilöiden seuraamiseen ei tulisi kuitenkaan käyttää esimerkiksi käyttäjän näppäimistön seurantaa muuten kuin yrityksen sääntöjen ja lain sen salliessa. Käyttäjiä tulisi myös informoida, jos sellaista seurantaa harjoitetaan (Krutz R, Russel V 2010, 145, 146).

Virtualisointi vaarantaa järjestelmät uudenlaisille uhkille samalla kun ne ovat alttiita samoille uhkille kuin perinteiset järjestelmät. Virtuaalisessa ympäristössä toimivat kaikki tunnetut hyökkäystavat. Virtuaalisointi on erillinen järjestelmä jota tulee suojata ja hypervisor on riskitekijä. Erillisten järjestelmien muuttaminen virtuaalisiksi lisää riskejä (Krutz R, Russel V 2010, 147).

Virtualisointi lisää järjestelmien monimutkaisuutta lisäten huomattavasti mahdollisuutta sopimattomiin konfiguraatioihin tai tähän mennessä tuntemattomille uhille. Hyökkääjä voi myös hyökätä virtuaalikonetta vastaan käyttämällä alempia käyttöoikeuksiaan päästäkseen sisälle virtuaalikoneeseen, minkä jälkeen korottaa oikeuksiaan hyökätäkseen järjestelmää vastaan hypervisorin kautta. Myös virtuaalijärjestelmät, jotka eivät ole käytössä ovat turvallisuusuhkia. Sellaiset järjestelmät voivat sisältää sensitiivistä tietoa ja niiden pääsynhallinta voi olla mahdotonta, mutta ne ovat turvallisuusuhkia, jos pääsy niihen estyy. Myös tehtävät ja vastuut pitää erottaa kunnolla virtuaalisessa ympäristössä. Mikäli käyttäjärooleja ei ole määritelty tarkasti, on se turvallisuusuhka. Koska virtuaalikone antaa pääsyn moniin komponentteihin, voi kunnollinen vastuiden hallinta olla hankala säilyttää. Virtuaalijärjestelmän hypervisor sisältää pääsyn fyysisten komponenttien tasolle ja tämä sisältää uuden uhan virtuaalijärjestelmälle. Täten hypervisor voi altistaa verkon uhkille huonosti suunnitellun pääsynhallinnan kautta, riittämättömän päivittämisen ja liian vähäisen monitoroinnin kautta. Tämä uhka pätee myös virtualisoituihin tietokantoihin (Krutz R, Russel V 2010, 147).

6 Pilvipalveluiden turvaaminen

Pilvipalveluiden turvaaminen alkaa palvelun tuottamiseen käytettävän tilan fyysisestä turvallisuudesta. Tilan fyysinen turvallisuus on aivan yhtä tärkeää, kuin mikä tahansa muu turvallisuustekijä millä pilvipalveluista pyritään tekemään turvallista. Fyysiset laitteet, kuten palvelimet ja tallennuslaitteet, ovat haavoittuvia fyysisille uhille mukaanlukien luonnonilmiöt, inhimilliset virheet ja katastrofit. Fyysisen turvallisuuden vamistamisella pyritään estämään asiaton pääsy tilaan jossa palvelua tuotetaan, tilassa oleviin resursseihin ja resurssien sisältämään tietoon. Fyysistä turvallisuutta tulisikin katsoa järjestelmien suojaamisena, jossa yksittäiset turvallisuuselementit tukevat toisiaan monitasoisessa suojauksessa. Nämä tasot ottavat huomioon asioita ympäristön suunnittelussa, pääsynhallinnassa, monitoroinnissa, henkilöiden tunnistuksessa ja tunkeilun tunnistamisessa. Jos näitä suojaustasoja rikotaan voi vastineena olla valojen, porttien tai lukitusalueiden käyttöä (Vic W 2011, 92).

Fyysisen turvallisuuden kaikki tasot tulisi integroida automaattiseen kontrollointiin ja valvontakeskukseen. Lisäksi tätä tukemaan tulisi palkata osaavaa ja hyvin koulutettua ammattimaista henkilökuntaa. Henkilökunnan tulisi olla omistautunut fyysisten resurssien suojaamiseen ja fyysisten turvallisuusprosessien säilyttämiseen myös katastrofitilanteissa (Vic W 2011, 92).

Pilvipalveluiden kehittämisestä sen operointiin asti tulisi käyttää turvallisuusstandardeja. Palveluiden eri osien tulisi sisältää oma standardinsa. Pääsynhallinnan osalta on tärkeää ymmärtää, että sitä käytetään ohjaamaan fyysistä pääsyä tilaan jossa palvelua tuotetaan. Pääsynhallinta rajaa myös loogista pääsyä järjestelmiin ja ohjelmistoihin. Välikohtauksiin reagointi ja hallinta on myös oma alueensa johon tulisi soveltaa standardia. Sen tulisi esittää kaikkien tahojen roolit ja vastuut aina välikohtauksen havainnoinnista sen jälkeiseen raportointiin. Myös järjestelmien ja verkkokonfigurointien varmuuskopiointi on hyvin tärkeää. Kaikkien palvelinten, kytkimien ja ylläpidettävien järjestelmien konfiguroinneista tulee pitää varmuuskopioita. Pilvipalveluntarjoajan tulee suorittaa ja dokumentoida turvallisuustestausta. Standardin tulisi sisältää eri henkilöiden roolit ja vastuut sekä tiedon milloin kolmannen osapuolen turvallisuustestaus tai arvio tulee suorittaa. Pilvipalveluiden tuotannossa tulisi aina käyttää hyväksyttyjä salakirjoitusalgoritmeja sekä hyväksyttyjä avainpituuksia. Salakirjoitusta tukemaan tulisi asettaa salasanastandardi. Standardin tulisi määrittää minkälainen salasana on hyväksyttävä. Se voi määritellä esimerkiksi sen pituutta ja rakennetta. Standardi voi myös määritellä kuinka palveluntuottaja testaa salasanan yhteensopivuutta standardin kanssa. Palvelua tulisi myös jatkuvasti monitoroida. Monitorointi määrittää kuinka muutokset suoritetaan tukemaan turvallisuuden perustasoa sen ollessa sen muuttuessa ja päivittyessä (Vic W 2011, 93, 94).

Identiteetin suojaaminen on tärkeää pilvipalveluissa ja sille voidaan asettaa vaatimuksia. Palveluntarjoajan tulee asettaa kontrollit suojaamaan identiteettitietojen luottamuksellisuutta, eheyttä ja saatavuutta. Palveluun tulee integroida ominaisuus, joka tunnistaa palvelun käyttäjät. Käyttäjä tulee tunnistaa rekisteröintivaiheessa lakivaatimusten mukaisesti. Käyttäjien tunnistettavuus tulee säilyä myös käyttäjän poistuessa palvelusta tulevaisuuden mahdollisia tutkimuksia varten. Kun käyttäjätunnuksia kierrätetään vanhoilta käyttäiltä uusille tulee huolehtia ettei vanhojen käyttäjien tietoa tai henkilökohtaisia tietoja siirry uudelle käyttäjälle. Täten voidaan huolehtia ettei käyttäjien henkilöllisyyksiä kierrätetä, vaan ainoastaan heidän pääsyoikeuksiaan järjestelmään (Vic W 2011, 95).

Järjestelmille jotka sisältävät asiakastietoja, ohjelmistoille ja verkkolaitteille tulee asettaa omat kontrollinsa. Niiden tulee käsittää kaikki fyysiset ja virtuaaliset ratkaisut. Turvallisuuskomponenteille tulee varmistaa riittävä eristäminen, konfigurointi ja turvallisuus. Verkko tule jakaa osiin ja ne tulee eristää toisistaan. Verkkojen turvallisuutta voi vahvistaa käyttämällä erilaisia verkkokontrolleja sekä palomuureja laitteissa. Ihmistä jolla on pääsy fyysisiin komponentteihin tulisi estää pääsy virtuaalikoneelle ja myös vastakkainen pääsy tulisi estää. Myös eri virtuaalikoneita, joilla on vastuu eri asiakkaan palveluiden suorittaminen, tulisi estää pääsemästä käsiksi toistensa tietoihin. Tulee myös huolehtia riittävistä kontrolleista, jotka takaavat käyttöjärjestelmien, virtuaalikoneiden, ohjelmistojen, verkkokonfiguraatioiden ja kaikkien asiakasohjelmistojen ja tietojen eheydestä. Palveluntarjoajan tulee myös huolehtia ohjelmisto ja järjestelmäpäivitysten eheydestä ennen niiden jakelua tuotantoon (Vic W 2011, 99, 100).

Yksittäiset turvallisuuskontrollit ovat yleensä riittämättömiä palvelun kokonaisvaltaiseen turvaamiseen. Siksi turvallisuuden varmistamiseksi on hyvä käyttää eri kerroksia jolloin riskien suuruutta voidaan vähentää minimiin. On viisasta suunnitella järjestelmä toisiaan vahvistavista kontrolleista jolloin varmuus turvallisuudesta kasvaa. Esimerkiksi VPN yhteyden käyttäminen etäyhteyksiin on viisasta. Toiseksi VPN yhteys voidaan estää mikäli sapuva ip-osoite ei löydy hyväksyttyjen osoitteiden listalta. Näin tekemällä voidaan huomattavasti vähentää sattumanvaraisen internetliikenteen pääsyä yrityksen verkkoon, kuin että sitä päästettäisiin syvemmälle verkkoon ennen kuin sen huomattaisiin olevan epätoivottua. Kolmanneksi kerrokseksi voidaan käyttäjiä vaatia käyttämään vaihtuvaa koodia, jonka ylläpitäjä tekee sattumanvaraisesti. Tällaisen koodin käyttäminen vahvistaa käyttäjäntunnistamista (Vic W 2011, 103).

6.1 Tiedon turvaaminen pilvessä

Käyttäjillä on epäilyksensä tietojensa säilyttämisestä julkisessa tai hybridipohjaisessa pilvessä. Näiden epäilysten voidaan nähdä johtuvan kahdesta seikasta. Ensinmäinen syy on, että tiedon omistavalla taholla on vähemmän kontrollia tietoihinsa, kun sitä käsitellään

heidän tilojensa ulkopuolella. Toinen syy on, että tiedon omistavalla taholla on pelkoja pilvipalveluiden merkitsevän riskejä luottamukselliselle tiedolle (Vic W 2011, 125. 126).

Asiakas voi pyytää palveluntarjoajaansa säilyttämään dataansa jossakin tietyssä datasalissa. Jos palveluntarjoaja suostuu tähän pyyntöön tulisi myös pyytää, että he ovat sitoutuneet noudattamaan paikallisia yksityisyyslakeja. Jokaisella palveluntarjoajalla on omat tapansa säilyttää dataa ja siksi olisi hyvä tuntea oman palveluntarjoajan tavat ylläpitää datan segregaatiota. Tulisi myös selvittää kenellä on erityisoikeudet dataanpääsylle. Mitä enemmän asiakas tietää palveluntarjoajansa tavoista, sen parempi (Sosinsky 2011, 260).

On selvää, että tiedon tulee olla turvassa asiattomalta käytöltä, kun sitä säilytetään sen omistavan organisaation ulkopuolella. Kun tietoa siirretään pilveen tulee sen olla aina salatussa eli kryptatussa muodossa, jolloin sen lukeminen on mahdotonta tai ainakin hyvin vaikeaa ilman oikeaa salausavainta. Tiedon kuljettamiseen voidaan käyttää myös välityspalvelinta. Näin tiedon hyödyntäminen kolmannen osapuolen toimesta tulee hyvin hankalaksi. Pelkkä tiedon kuljetus kryptatussa muodossa ei riitä, se tulee myös säilyttää siten.

Vahva tiedonsalaaminen on tärkeä tekniikka, jota käytetään tiedon siirrossa ja säilytyksessä. Salaamisen tarkoitus on synnyttää virtuaalisia säilytystilaa, joka ylläpitää tiedon luotettavuutta ja muuttumattomuutta säilyttäen samalla pilvipalvelun edut: kaikkialla läsnäolevan, luotettavan ja jaetun datavaraston. Vaikka salaaminen suojaa tietoa asiattomalta pääsyltä, se ei kuitenkaan suojaa mitenkään datanhävittämiseltä. Salausavainten hukkaaminen on yleisin syy datan hukkaamiselle. Salausavaimilla tulisi olla tietynpituinen elinkaari. Avainten suojaamisen lisäksi tulisi olla turvallisia avainten säilytysvarastoja, joihin on tiukka rooleihin perustuva pääsy, automaattinen varmuuskopiointi ja palautustavat. Avaintenhallinta olisi hyvä erottaa pilvipalveluntarjoajasta. (Sosinsky 2011, 260).

Tietojärjestelmistä tulisi aina väliajoin ottaa varmuuskopio johon voidaan palata järjestelmän tarvitessa palautusta toimivaan tilaan. Tällaisen systeemikuvan ottaminen ja kyky sen analysointiin on kullanarvoista. Tällainen varmuuskopio sisältää kopion koko järjestelmästä mukaanlukien ohjelmistot ja datan, verkkoasetukset, palomuurit sekä kytkinkonfiguraatiot. Käyttämällä varmuuskopiota järjestelmän ollessa uhattuna voidaan ongelma saada haltuun (Sosinsky 2011, 250, 251). Varmuuskopioita ei tulisi säilyttää vain pilven sisällä tai yhdessä pilvessä. Kaikkien palveluntarjoajien palvelut ovat joskus saavuttamattomissa. Tällöin palveluiden jatkuvuussuunnittelu nousee tärkeään osaan. Palvelunlaatua voidaan varmistaa SLA-tyyppisellä sopimisella, mutta tulee muistaa sen olevan aina kallimpaa kuin ilman sopimusta tuotettava palvelu. Vaihtoehto tälle on monistaa palvelut useampaan palvelinkeskukseen. Tällöin kokonaissaavutettavuus voi nousta tavallista korkeammalle, mutta samalla kuitenkin otetaan riski luottamuksellisuuden suhteen (Nixu 2010, 8.)

Tärkeimmät seikat datan turvaamiseen pilvessä ovat: pääsynhallinta, auditointi, autentikointi ja autorisointi. Käytettiinpä mitä tahansa pilviapalvelumallia tulisi turvatoimien käsittää nämä neljä seikkaa. Tavallisesti tiedonturvaamiseen it-järjestelmissä on käytetty palomuuria, mutta pilvipalveluissa ei ole fyysistä järjestelmää, joka hoitaisi sen virkaa. Tämän takia tulisi data eristää suoralta asiakaspääsyltä. Yksi tapa tehdä tämä on käyttää eri kerrostettua pääsyä dataan. Tässä tapauksessa käytetään välittäjää ja välityspalvelinta, jolloin asiakas ottaa yhteyden välityspalvelimen kautta välittäjään, jolla on pääsy dataan. Välittäjä tuo datan valityspalvelimelle, joka ohjaa datan asiakkaalle. Välityspalvelimella ei ole pääsyä dataan, mutta sillä on pääsy asiakkaaseen ja välittäjään. Välittäjällä taas ei ole pääsya asiakkaaseen, mutta täysi pääsy dataan (Sosinsky 2011, 256, 257.)

Auditointi on hyvin tärkeää, jotta voidaan selvittää mitä on tapahtunut. Se on erityisen tärkeää, kun selvitetään rikkeitä. Auditointi perustuu lokeihin tapahtumista. Lokien tulisi tallentaa ainakin järjestelmän, ohjelmistojen ja turvallisuusasioiden tapahtumat. Palveluntarjoajalta voidaan pyytää selvitystä ovatko he valmiita kohdistamaan toimintaansa ulkopuolisen auditoinnin alle. Mikäli he eivät ole halukkaita avamaan toimintaansa ulkopuolisen tarkastettavaksi, on viisasta käyttää toista tarjoajaa tai käyttää heidän palveluitaan siten, että riskit omalle toiminnalle on minimaalista. Esimerkiksi sensitiivisen tiedon säilytystä kyseisenkaltaisella tarjoajalla tulisi välttää, vaikka he salaisivat tiedon asianmukaisesti. Organisaatio, joka käsittelee tietoa on vastuussa, että tiedonsäilyttäminen on lakien ja säädösten muikaista. Tähän ei tee poikkeusta se, että tiedon säilyttämiseen käytetään ulkopuolista palveluntarjoajaa. Tiedon omistaja on vastuussa tiedon turvallisesta säilyttämisestä ja ettei tiedon eheys ole kärisnyt. (Sosinsky 2011, 261, 262.)

6.2 Turvamenettelyt datan suojaamiseksi

Kaikkien riskiskenaarioiden käsittely ei ole mahdollista, joten organisaatioiden tulisi omaksua riskeihin perustuva lähestymistapa pilvipalveluihin ja turvallisuusvaihtoehtojen valintaan. Mikään lista turvallisuuskontrolleista ei vastaa kaikkiin turvallisuushaasteisiin, sillä pilvipalvelumalleja on niin useita: julkinen -tai yksityinentuotanto, sisäinen -tai ulkoinenisännöinti sekä useat hybridimuunnelmat. Aina datalle ei kuitenkaan edes kannata tuottaa monimutkaisia suojauksia. Silloin kyseessä on vähäarvoinen data, jonka paljastuminen ei tuota merkittäviä haittoja. Tilannetta voisi verrata kriittiseen sovellukseen, jota ei kannata välttämättä siirtää julkiseen pilveen sen tärkeyden takia (CSA 2011, 8.)

Datanturvaamisella on oma elinkaarensa ja se alkaa datan luonnilla ja päättyy sen mahdolliseen tuhoamiseen. Kaikkea dataa ei välttämättä tuhota. Kun uutta digitaalista sisältöä luodaan se sijoitetaan seuraavaksi säilytettäväksi johonkin tallennustilaan. Säilyttäminen on sitoutumista digitaalisen datan säilyttämiseen jossakin säilytysrepositiossa. Usein säilytys alkaa samanaikaisesti luonnin kanssa. Dataa voidaan ottaa säilytyksestä käyttöön jolloin sitä prosessoidaan tai käytetään muilla tavoin, poislukien muokkaus. Dataa

voidaan jakaa eriosapuolille, kuten asiakkaat tai muut käyttäjät. Kun data ei ole enää aktiivisessa käytössä, se arkistoidaan pitkäaikaiseen tallennustilaan. Viimeiseksi data tuhotaan fyysisesti tai digitaalisesti eli ylikirjoittamalla (CSA 2011, 53.)

Tietoturvallisuus pilvipalveluiden osalta voidaan jakaa kolmeen osaan: datan migrointi pilvipalveluun, datan suojaaminen sen ollessa liikkeessä pilvipalveluun tai eri ympäristöön ja datan suojaaminen sen ollessa pilvessä. Tavallisesti datansuojaaminen käsittää pääsynhallinnan ja salakirjoittamisen, mutta on lisäksi kaksi muuta tapaa suojata hyväksymättömän datan siirtyminen pilveen. Ensinmäinen näistä on suurten datamäärien migroinnin tarkkailuun tarkoitetut tietokantojen aktiivisuuden monitorointi (DAM) sekä tiedostojen aktiivisuuden monitorointi. Toinen tapa on monitoroida datan liikkumista pilveen URL suodatuksella ja datan häviämisen estämisellä (DLP) (CSA 2011, 55.)

Tunkeilijan havaitsemisjärjestelmä tai murron estämisjärjestelmä (IDS, IPS) ovat molemmat tärkeitä verkon turvallisuutta parantavia asioita. Ne monitoroivat käytösmalleja käyttämällä sääntöihin pohjautuvia tai heuristisia tai käytökseen perustuvia malleja havaitakseen erikoisuuksia toiminnassa, jotka voisivat olla uhkia yritykselle. Ne ovat suosittuja, koska niiden avulla voidaan nähdä mitä yrityksen verkossa tapahtuu. IDS ja IPS ratkaisut monitoroivat verkkoliikennettä ja vertaavat aktiivisuuta asetettuun vertailukohtaan sääntöpohjaisesti tai statistiikka-analyysin avulla. IDS monitoroi verkkoa passiivisesti keskittyen sensitiivisiin verkon osiin. IPS puolestaan on aktiivisempi puolustaessaan verkkoa tunkeilua vastaan (CSA 2011, 167.)

Ennen kuin dataa voidaan siirtää pilveen pitää se ensin irroittaa aiemmasta repositiostaan. Tietokannan aktiivisuuden monitorointi voi auttaa havaitsemaan jos pää -tai muukäyttäjä irroittaa suuren määrän dataa, sellainen voi indikoida migraatiota. Tiedostojen aktiivisuuden monitorointi antaa samanlaista suojaa, mutta tiedostorepositioille. URL suodatuksella voidaan estää käyttäjiä yhdistymistä verkon kautta pilvipalveluihin. DLP työkalut katsovat datan sisältöä eivätkä vain sen määränpäätä, ja ovat siksi tehokkaampia suojausmenettelyitä kuin URL suodatus. Niiden avulla käyttäjä voi estää tietynkaltaisen datan siirtymistä pilveen. Esimerkiksi arkaluontoisen materiaalin voidaan sallia siirtyvän hyväksyttyyn palveluun, mutta estää sen siirtyminen palveluun jota ei ole hyväksytty (CSA 2011, 56.)

Pilvipalveluissa on aina tärkeää suojata dataa kun se on liikkeessä, oli kyse sitten julkisesta tai yksityisestä palvelusta. Myöskään erilaiset palvelumallit eivät tuo liikkumavaraa tähän suojausmenettelyyn. Datan suojaamiseen sen ollessa liikkeessä liittyy seuraavat seikat. Ensinmäinen tekijä on: datan liikkuminen tavanomaisista infrastruktuureista pilvipalveluihin, mukaanlukien julkiset/yksityinen, sisäinen/ulkoinen ja muut permutaatiot. Toiseksi tekijäksi voidaan ottaa datan liikkuminen pilvipalveluntarjoajien välillä ja kolmanneksi datan liikkuminen eri instanssien välillä tietyn pilven sisällä (CSA 2011, 56.)

Datan suojaamiseen näissä tapauksissa on kolme vaihtoehtoa. Näistä ensinmäinen on datan salakirjoittaminen ohjelmallisesti ennen kuin se lähetetään verkonkautta vastaanottajalle. Tämä voi tapahtua esimerkiksi palvelimella. Toinen vaihtoehto on verkkotasolla tapahtuva salakirjoitus. Tällöin salakirjoitukseen käytettäisiin standardinomaisia ratkaisuita kuten SSL, VPN tai SSH. Salakirjoittaminen voi tapahtua rauta -tai ohjelmistopohjaisesti. Kolmas, mutta ei aina suositeltu tapa on lähettää salakirjoitettava data erilliselle salakirjoitusohjelmalle tai palvelimelle ennen kuin se lähetään verkossa eteenpäin. Tätä tapaa käytetään erityisesti, kun integroidaan vanhoihin ohjelmistoihin (CSA 2011, 56, 57.)

Lähteet

Painetut lähteet

Baun C, Kunze M, Nimis J, Tai S, 2011 Cloud computing. 2. painos. Springer-Verlag Berlin Heidelberg

Marks E, Lozano R, 2010 Executive's Guide to Cloud Computing.

Ronald K, Russel V, 2010 Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, Indiana: Wiley publishing.

Sosinsky, B 2011 Cloud computing bible. Indianapolis, Indiana: Wiley publishing. John Wiley & Sons. Hoboken, New Jersey.

Sähköiset lähteet

Boroujerdi M, Nazem S 2009 World Academy of Science, Engineering and Technology 34 2009. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.309.1337&rep=rep1&type=pdf Viitattu 29.11.2015

European Data Protection Supervisor https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA10. Viitattu 29.11.2015