Pilvipalvelut ja tietoturva

Marko Leppänen

Opinnäytetyö
Toukokuu 2013
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

MARKO LEPPÄNEN:
Pilvipalvelut ja tietoturva

Opinnäytetyö 37 sivua
Toukokuu 2013

Pilvipalvelut ovat verkon välityksellä tarjottavia sovelluksia ja laitteistoresursseja palveluna. Palveluntarjoaja hoitaa laitteiden ja sovellusten ylläpidon, päivittämisen ja tietoturvan, jolloin asiakas voi keskittyä omaan liiketoimintaansa. Sen piirteitä ovat skaalatutuvuus, helppo hallittavuus, saatavuus ajasta ja paikasta riippumatta. Jos palvelut ovat kaupallisia, maksu perustuu käyttäjien tai käytettyjen resurssien määrään.

Työn yksi tavoitteista oli antaa pilvipalveluita harkitseville yrityksille kattava yleiskuva saataville olevista palvelutyypeistä ja kertoa mihin niitä käytetään. Palvelut voidaan jakaa kolmeen eri malliin: infrastruktuuri, sovellusalusta ja sovellukset palveluna. Julkisien pilvipalveluiden lisäksi yritykset voivat luoda omia yksityisiä pilvipalveluita omiin tai vuokrattaviin palvelintiloihin tai perustaa muiden organisaatioiden kanssa yhteisöpilven. Etenkin julkisiin pilvipalveluihin siirtymiseen liittyy myös riskejä, kuten uudet tietoturvauhat ja pelko palvelun saatavuusongelmista.

Työssä arvioidaan pilvipalveluita käyttävien yritysten etuja ja riskejä verrattuna paikallisten IT-resurssien käyttöön sekä perehdytään tarkemmin pilvien suurimpana pidettyyn ongelmaan eli tietoturvaan. Nopeasti kehittyvissä pilvipalveluissa tietoturva laahaa aina hieman perässä, koska uusien palveluiden syntyessä syntyy myös väistämättä uusia tietoturva-aukoja. Tietovuodon tapahtuessa syy on harvoin palveluntarjoajan päässä, vaan yleisin syy on asiakasorganisaation työntekijöiden huolimattomuus tai tietämättömyys tietoturva-asioissa. Tässä opinnäytetyössä käydään läpi suurimmat tietoturvauhat, joita yritys voi kohdata pilvessä sekä esimerkkitapauksia ja ohjeita ongelmien torjumiseen.

Asiasanat: pilvipalvelut, pilvilaskenta, tietoturva

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunications Engineering and Networks

MARKO LEPPÄNEN:
Cloud Services and Security

Bachelor's thesis 37 pages
May 2013

Cloud services are applications and hardware resources which are accessible via a network as a service. Service provider handles maintaining, updating and security of these resources, allowing customers to focus on their core business. Resources of the cloud should always be available when needed, scalable and easily manageable. If services are commercial, costs are based on subscription or consumption depending on the service model.

This thesis aims to give companies considering moving to cloud a comprehensive overview of available types of services, and explain the reader for what those can be used. Cloud services can be divided into three different categories: infrastructure, platform and application as a service. Besides of public cloud services companies can create own private clouds to their own or rented servers or establish shared community cloud with other organizations. The transition to cloud services adds new risks such as security threats, uptime and availability issues.

Study evaluates the benefits and risks of cloud services compared to local servers, and takes a closer look at security which is ranked first as the greatest challenge or issue of cloud services. Rapid emerging of cloud computing causes security problems, as new services arise, inevitably new vulnerabilities will also occur. When information leakage happens, the cause is rarely service providers. The most common cause is a client user's negligence or unawareness about security matters. This thesis will walk you through the biggest security threats which company may face in the cloud, as well as examples and guidelines to tackle these problems.

Key words: cloud services, cloud computing, security

SISÄLLYS

LYHENTEET JA TERMIT

AMI	Amazon Machine Image
API	Application Programming Interface, ohjelmointirajapinta jonka kautta ohjelmat voivat kommunikoida keskenään
AWS	Amazon Web Services, Amazonin pilvipalvelut
CSA	Cloud security alliance
DDoS	Distributed Denial of Service, Hajautettu palvelunestohyökkäys
DoS	Denial of Service, palvelunestohyökkäys
GPU	Graphics Processing Unit, Grafiikkaprosessori
Hypervisor	Virtualisoinnissa käytetty ohjelmisto komentojen välittämiseen virtuaalikoneesta laitteistolle
IaaS	Infrastructure as a Service, tietotekniikan infrastruktuuri palveluna
Klusteri	Malli, jossa yksi kone jakaa laskentatyötä useamman koneen kesken.
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service, alusta palveluna
QoS	Quality of Service, laatulupaus
S3	Simple Storage Service, Amazonin pilvitallennuspalvelu
SaaS	Software as a Service, Ohjelmisto palveluna
SLA	Service Level Agreement, palvelutasosopimus
URI	Uniform Resource Identifier, merkkijono resurssien identifioimiseksi, joka muodostuu nimestä (URN) ja osoitteesta (URL)
Valtuustieto	Hyväksytystä sisäänkirjautumisesta saatu todistus.
Xen	Ilmainen ja vapaa virtualisointiohjelmisto
XSS	Cross-site scripting, sivustojen välinen komentosarjahyökkäys

1 JOHDANTO

Pilvipalveluiden suosio on edelleen kasvussa ja huolimatta monien skeptisyydestä ideaa kohtaan alkuaikoina, pilvipalvelut ovat tulleet jäädäkseen niin organisaatioiden kuin yksityistenkin käyttöön. Suosittuja pilvitoimintamalliin perustuvia palveluita kuten Facebook ja Gmail käyttävät monet tietämättään koko pilvipalvelu käsitteestä. Ideana pilvipalvelu on kuitenkin jo vanha keksintö, mutta vielä edelleen termi on pääpiirteitä lukuun ottamatta hatara useiden eri määrittelyiden takia. Seuraavissa kappaleissa tullaan käsittelemään aiheen keskeinen sisältö, kuten pilvipalveluiden eri mallit, arkkitehtuurit, hyödyt ja haitat pilvipalveluihin siirtymistä harkitsevien organisaatioiden näkökulmasta.

Pilvipalvelut ovat laaja ja etenkin viime vuosina hyvin suosittu aihe, josta on kirjoitettu jo lukuisia opinnäytetöitä ja muita teoksia. Tässä työssä kuitenkin perehdytään yleisen pilvipalvelumallin esittelyn lisäksi syvemmin sen tietoturvaan, jota pidetään pilvipalveluiden suosion suurimpana haasteena. Tietoturvan kannalta pilvipalveluissa on etunsa ja riskinsä, mutta oikein suunniteltuna ja tehtynä pilveen siirtyminen ei välttämättä kuitenkaan laske tietoturvatasoa paikalliseen palvelinratkaisuun nähden. Työssä käydään läpi suurimmat Cloud Security Alliancen määrittämät tietoturvauhat, joita yritys voi kohdata pilvessä sekä esimerkkitapauksia ja vinkkejä ongelmien torjuntaan.

Pilvipalvelut eivät ole automaattisesti avain menestykseen, vaan niistä saatavat hyödyt riippuvat suuresti yrityksen IT-tarpeiden tyypistä. Tässä opinnäytetyössä on pyritty puolueettomasti esittämään pilvipalveluiden tarjontaa sekä auttamaan pilveen siirtymistä harkitsevaan yritystä päätöksen teossa. Aiheisiin on myös kerätty varoittavia tutkimustuloksia ja esimerkkitapauksia pilvipalveluista ja sen tietoturvavaaroista.

2 PILVIPALVELUN MÄÄRITELMÄ

Pilvipalvelu on terminä hyvin uusi, mutta ideana vanhempi kuin itse internet. Vuonna 1969 J.C.R. Lickliderin visio globaalista järjestelmästä, johon kaikki yhteydessä olevat pääsisivät kiinni ohjelmiin ja dataan paikasta riippumatta, muistutti suuresti nykyajan pilvipalveluita. (Arif 2009) Termiä pilvipalvelu eli cloud computing kuultiin ensimmäistä kertaa käytettävän Googlen tämän hetkisen pääjohtaja Eric Schmidt vuoden 2006 Search Engine Stragies –konferenssissa. (Mustonen 2011, 12)

Termille pilvipalvelu ei ole saatu hyväksyttyä yhtä yhteisesti määritelmää. Monet alalla toimivat yritykset ovat antaneet näkemyksensä siitä mitä pilvipalvelut heidän mielestänsä sisältävät. Yleisellä tasolla pilvipalveluilla tarkoitetaan mallia, jossa sovellukset, talletus- ja laskentakapasiteetti, tietoliikenneyhteydet ja palvelut tarjotaan verkon kautta käyttäjälle ilman, että hänen tarvitsee tietää resurssien sijaintia, tai huolehtia niiden ylläpidosta ja toiminnasta. (Salo 2010, 12)

2009 vuoden OSCON-konferensissa Canonicalia edustava Simon Wardley kertoi esityksessään löytäneensä 67 eri määritelmää pilvipalveluille ja että uusia syntyy kuin sieniä sateella. Wardley itse määrittelee pilvipalvelut seuraavasti: ”Pilvipalvelut
on yleinen käsite kuvaamaan informaatioteknologiassa meneillään olevaa muutosta,
jonka suuntana on palveluihin perustuva toimintamalli ja muutosta ajavina voimina
taloudelliset, kulttuuriset ja teknologiset olosuhteet.” Hänen mukaansa on tapahtumassa suuri murros, joka muuttaa tapaa jolla tietotekniikkaa käytetään. (Salo 2010, 12)

Lama-aika on ollut hyväksi pilvipalvelumallien kasvulle. Vapauttamalla yrityksiä talouden laskukausina ei-toivotuilta IT-investoinneilta, pilvipalvelut ovat pystyneet kasvattamaan suosiotaan maailmanlaajuisesta finanssikriisistä huolimatta. Pilviratkaisuun siirtyvät yritykset ovat muuttaneet kulurakennetta kiinteistä kustannuksista muuttuviin. (Salo 2010, 12)

Yhtenä virallisimpana määritelmänä voidaan pitää NISTin (National Institute of Standards and Technology) antamaa määritelmää pilvipalveluille. NIST toimii Yhdysvalloissa julkishallinnon standardeja suunnittelevan elinkeinoministeriön alaisena ja määrittelee pilvipalvelun seuraavasti: ”Cloud Computing on toimintamalli, joka mahdollis-

taa pääsyn vapaasti konfiguroitaviin ja skaalautuviin tietotekniikkaresursseihin, jotka voidaan ottaa käyttöön ja poistaa käytöstä helposti ja nopeasti.” (Salo 2010, 12)

NIST antaa määritelmässään pilvipalveluiden viisi ominaispiirrettä:

1. On-demand itsepalvelu
   Käyttäjä säätelee tietotekniikkaresursseja itse ilman, että hänen on oltava yhteydessä palveluntarjoajan henkilöstöön. On-demand tarkoittaa, että resursseja voidaan ottaa käyttöön kun niitä tarvitaan ja vastaavasti vähentää tai poistaa kokonaan kulujen vähentämiseksi.

2. Pääsy palveluihin eri päätelaitteilla
   Palvelut ovat käyttäjän ulottuvilla usealla eri päätelaitetyypillä, kunhan laite on kytkettynä verkkoon. Käyttö voi tapahtua kannettavalla tietokoneella, työasemalla, taulutietokoneella kuin älypuhelimellakin.

3. Resurssien yhteiskäyttö
   Palveluntarjoajan resurssit ovat yhdistetty isoiksi kokonaisuuksiksi, joista asiakkaille jaetaan resursseja tarpeen mukainen osa. Käyttäjällä ei ole yleensä ole tietoa siitä missä ja millä tavalla palvelut toimivat. Useat asiakkaat saattavat käyttää samoja resursseja yhteisesti toisistaan riippumatta ja tietämättä. Resurssit voivat olla esimerkiksi tallennustilaa, laskentatehoa, muistia tai verkkokaistaa.

4. Nopea joustavuus
   Palveluita voidaan nopeasti varata lisää tai vapauttaa käytöstä, joissain tapauksissa myös automaattisesti. Käyttäjän näkökulmasta resurssit näyttävät usein äärettömiltä ja niitä voidaan ottaa käyttöön rajattomasti milloin vain. Tämä mahdollistaa yritysten valmiuden suunnittelemattomien resurssitarpeiden muutoksiin kuten tallennus-, laskenta- ja tietoliikennekapasiteetin lisäämiseen välittömästi tarpeen esiintyessä.

5. Käytön mittaaminen
   Asiakasta laskutetaan resurssien käytön mukaan, joten järjestelmä mittaa ja valvoo tarkasti palveluiden käyttöä. Myös asiakas pääsee käsiksi omasta käytöstä kerättyyn informaatioon. Informaatio voi sisältää esimerkiksi käytetyn tallennus-

tilan, verkkokaistankäytön tai aktiivisten käyttäjätilien määrän. (Mell & Grance 2011, 2)

3 PILVIPALVELUMALLIT

3.1 IaaS

Infrastruktuuri palveluna eli Iaas (Infrastructure as a Service) on virtuaalinen palvelinkeskus pilvessä. IaaS-palveluntarjoaja tarjoaa asiakkaalle prosessointitehoa, tallennustilaa, muistia, kuormantasaajia, verkkoyhteydet ja muita tietokoneresursseja. IaaS:n erot verrattuna normaaliin ulkoistamiseen ovat resurssien yhteiskäyttö, joustavuus, itsepalvelu, automaattisuus ja resurssien käytön mukaan tapahtuva laskutus. Palveluntarjoajan laitteiden kapasiteetti on usein virtualisoitu parhaan tehohyödyn saavuttamiseksi. Virtualisoitu kapasiteetti skaalataan asiakkaan tarpeiden mukaan. Skaalaus säätelee asiakkaalle annettavan kapasiteetin määrää sen tarpeen mukaan automaattisesti. Näin ollen vapautuva kapasiteetti voidaan ohjata toisen asiakkaan käyttöön.

Pilvettömässä ratkaisussa tyypillinen sovellus käyttää vain pienen osan palvelinten kokonaislaskentakapasiteetista, mutta kuormahuippujen takia kapasiteetti on mitoitettava suuremmaksi. Tällöin laitteiston kapasiteettia menee hukkaan. Pilvessä useampi käyttäjä jakaa saman laitteiston ja on täten epätodennäköisempää, että kuormahuiput osuisivat samalla hetkellä. Pilvessä sijaitsevien virtuaalikoneiden eli instanssien lukumäärää voidaan tyypillisesti muuttaa lennosta muutoksien tullessa voimaan minuuteissa. (Infrastructure as a Service 2011)

Verrattuna PaaS- ja SaaS-palveluihin infrasturktuuri palvelut ovat huomattavasti vapaampia. Laitteiden fyysistä muokkausta lukuun ottamatta käyttäjille saatetaan antaa hyvinkin vapaat kädet palveluntarjoajasta riippuen. Vapauden kääntöpuolena on suurempi vastuu. Palveluntarjoajan tehtävänä on huolehtia palveluiden toimivuudesta ja pitää samaa alustaa käyttävät asiakkaat toisistaan riippumattomina. Asiakkaan vastuulle jää ohjelmistojen toimivuus, päivitykset ja tietoturva.

Vuoden 2012 syksyllä IaaS:n osuus pilvipalvelumarkkinoista oli noin 45 % ja suosio on kasvussa (PaaS, IaaS ja SaaS: riskit ja suosio 2012). Tämän hetken ehdottomasti suurin IaaS-palveluntarjoaja on Amazon Web Services (AWS) . Amazon tarjoaa Xen-pohjaisia virtualisoituja infrastruktuureja. Yhtiöt kuten Verizon ja Baremetalcloud tarjoavat asiakkailleen virtualisoitujen instanssien sijasta fyysisiä palvelimia. (Burns 2012)

3.2 PaaS

PaaS eli sovellusalusta palveluna (Platform as a Service) on sovelluskehittäjille suunnattu pilvipalvelumalli, joka tarjoaa alustan sovellusten rakentamiseen, kehittämiseen, testaamiseen sekä ylläpitoon. IaaS:in tapaan PaaS-palveluun luotu sovellus on skaalattavissa käyttäjämäärän mukaan. Sovellusten rakennus palvelun avulla voidaan toteuttaa hyvin pienillä kustannuksilla. Kun valmis sovellus otetaan lopulta käyttöön, käyttäjämäärät ja kustannukset kasvavat, mutta tällöin myös tulot kasvavat. PaaS:n käyttö piilottaa infrastruktuurin, jolloin tarve yrityksen omalle IT-ylläpidolle vähenee. Pilven ansiosta sovellusta ei tarvitse pilkkoa eri palvelimille, vaan järjestelmä hoitaa skaalauksen automaattisesti. (Platform as a Service 2011)

Datan sijaitessa yrityksen palomuurin ulkopuolella huolena on kaikkien pilvimallien tapaan tietoturva. Vieraan alustan osaamisvaatimukset kehityksessä ja ylläpidossa ovat PaaS:n haasteita. Esimerkiksi Force.com-alustalla käytössä on vain Salesforce.comin oma Apex-ohjelmointikieli. Yksi PaaS-alustojen suurimmista ongelmista on lukittuminen valittuun palveluntarjoajaan. Alustojen rajapinnat, työkalut ja joissakin tapauksissa jopa ohjelmointikielet ovat yksilöllisiä, joka tekee palveluntarjoajan vaihtamisesta erittäin vaivalloista. Sovelluksen siirto palvelusta toiseen aiheuttaa todennäköisesti suuria muutoksia sovelluksen koodissa. Koska PaaS-sovellus on vahvasti sidottuna palveluntarjoajaan, pelkona on alustan ylläpidon loppuminen. (Platform as a Service 2011)

Osa tarjolla olevista PaaS-palveluista on tehty kolmannen osapuolen IaaS:n päälle, kuten Amazonin pilvipalvelimilla pyörivä Heroku. Heroku tarjoaa alustan Java-, Ruby-, Clojure-, Node.js-, Python- ja Scale-kielisille sovelluksille ja maksaa Amazonille asiakkaidensa käyttämästä laskentatehosta (Heroku 2013). Ylimääräisen välikäden vuoksi asiakkaalle saattaa tulla kalliimmaksi PaaS-ratkaisu kuin oman sovellusalustan rakentaminen IaaS-pohjalle.

PaaS:ia hyödyntävien organisaatioden määrä kolminkertaistui Suomessa vuoden 2012 aikana (Mäntysaari 2012). Vuoden 2012 syksyllä PaaS:n osuus globaaleista pilvipalvelumarkkinoista oli noin 10 % (PaaS, IaaS ja SaaS: riskit ja suosio 2012). Tunnetuimpia pilvipalvelupohjaisia sovellusalustoja ovat Googlen AppEngine, Salesforce.comin Force.com ja Microsoftin Windows Azure. Jokaisella palveluntarjoajalla on tietyt ennalta

määrätyt ohjelmointikielet, joita alusta tukee. Esimerkiksi AppEngine-alustalla voidaan ainoastaan käyttää Javaa, Pythonia tai Googlen omaa Go-ohjelmointikieltä (Google Developers 2013).

3.3 SaaS

SaaS-pilvipalvelumallissa (Software as a Service) palveluntarjoaja tarjoaa asiakkaalle ohjelman, ohjelmiston tai käyttöjärjestelmän verkon välityksellä. Palveluita käytetään tyypillisesti internetselaimen kautta, joten työskentely on periaatteessa mahdollista päätelaitteesta tai paikasta riippumatta. Tunnettuja esimerkkejä SaaS:sta ovat muun muassa sähköpostipalvelut kuten Gmail ja Outlook.com, sekä tiedontallennukseen käytettävät Dropbox ja Google Drive. Palvelusta veloitetaan perinteisen lisenssimaksun sijaan käyttöajan, kone- tai käyttäjämäärän mukaan. Saas-palveluita käyttämällä yritys voi vähentää laitteistoon ja ohjelmistoon sitoutuneen pääoman määrää. Päivityksien ja ylläpidon vähenemisen ansiosta vapautuu henkilöstöresursseja tuottavampiin tehtäviin. (Mustonen 2011, 18)

Palveluntarjoajan ylläpitotaakan helpottamiseksi SaaS-mallissa ylläpidetään vain yhtä sovellusta usean erillisen sijaan. Sama sovellus palvelee kaikkia asiakkaita heidän siitä tietämättä. Tälläinen monikäyttäjyys (multitenancy) mahdollistaa resurssien tehokkaan käytön ylläpitäjän kannalta.

SaaS on Suomen yleisimmin hyödynnetty pilvipalvelumalli, mutta suosio on hidastumassa. Vuoden 2012 syksyllä SaaS:n osuus globaaleista pilvipalvelumarkkinoista oli noin 45 %. (PaaS, IaaS ja SaaS: riskit ja suosio 2012)

Tyypillisiä SaaS-palveluita:

- Virtuaalinen Windows-käyttöympäristö tai työpöytä
- Kirjanpito-, varastonhallinta-, taloushallinta- ja verkkokauppasovellukset
- Teknisten piirustusten luonti ja levitys
- Dokumenttien luonti ja muokkaus
- Asiakashallintasovellukset
- Projektinhallintasovellukset
- Viestintäsovellukset.

4 PILVIPALVELUIDEN ARKKITEHTUURI

NIST on esittänyt neljä käyttöönottomallia: yksityinen pilvi, yhteisöpilvi, julkinen pilvi ja hybridipilvi. Palvelut ovat jaettu ryhmiin niiden omistajien ja saatavuuden mukaan.

Yksityisessä pilvessä palvelut toimitetaan organisaation omasta tai vuokratusta palvelinkeskuksesta ainoastaan organisaation yksityiskäyttöön. Tällä pyritään saavuttamaan pilvipalveluiden edut, kuten joustavuus, skaalautuvuus ja helppo käsiksi pääsy resursseihin. Yksityisyys tuo vapauden kontrolloida ja valvoa palveluita halutulla tavalla, sekä hyvin suunniteltuna mahdollistaa merkittävät kustannussäästöt. Markkinoille on viimevuosina tullut useita ohjelmistoja, joilla kuka tahansa voi pystyttää pilvipalvelun riittävällä palvelinlaitteistolla. VMwaren vSphere on pienille ja keskisuurille yrityksille suunnattu ohjelmistokokonaisuus pilviympäristön luontiin. Ohjelmiston avulla on mahdollista suorittaa täydellistä virtualisointia x86-pohjaisilla laitteilla (Mäkelä 2011, 30). Vastaavia ohjelmistoja on myös saavilla ilmaiseksi, kuten avoimen lähdekoodin Apache CloudStack ja OpenStack.

Yhteisöpilvi on yksityisen pilven kaltainen sillä erolla, että pilvipalvelinkeskus on useamman organisaation omistuksessa ja käytössä. Organisaatiot toimivat tyypillisesti tiiviissä yhteistyössä. (Mustonen 2011, 19) Julkiseen pilveen verrattuna tietoturva voidaan olettaa paremmaksi ja kustannukset pienemmiksi kuin yksityisessä pilvessä.

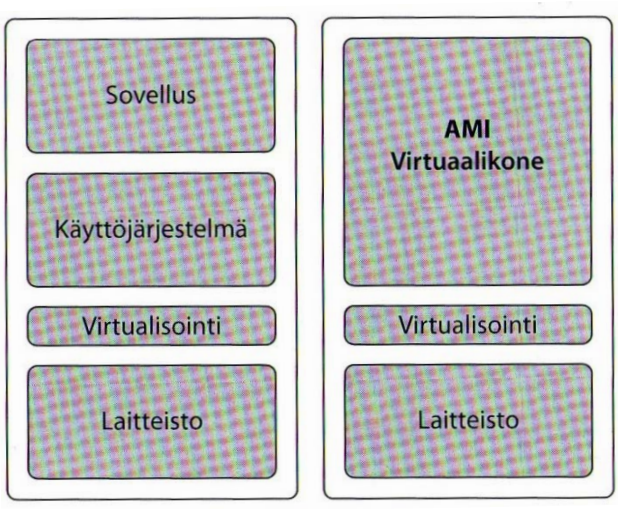
Julkinen pilvi palveluntarjoajan ylläpitämä pilvipalvelu, jota asiakas voi käyttää maksua vastaan. Palveluntarjoaja huolehtii laitteistosta, ohjelmistosta, hallinnoinnista ja palveluista. (Salo 2010, 19) Julkisia pilvipalveluita löytyy niin yksityisille henkilöille kuin yrityskäyttöönkin. Pilvimuoto on hyvä vaihtoehto julkiselle korkean saatavuuden tiedolle, mutta huono salassapidon kannalta

Hybridipilvi on NISTin määritelmän mukaan kahden tai useamman yllämainitun pilviarkkitehtuurin yhdistelmä. Hybridipilvelle on kuitenkin annettu myös toinen määritelmä. Sen mukaan hybridipilven yksi osa on palvelupilvessä ja toinen paikallinen ratkaisu. Esimerkiksi jos yritys on päättänyt varastoida osan tiedosta pilveen, mutta haluaa pitää tärkeimmät tiedostot omassa paikallisessa palvelinkeskuksessa. (Salmio 2012, 18)

5 VIRTUALISOINTI

Virtualisoinnilla on suuri merkitys pilvipalveluiden toiminnassa. Ilman virtualisointia pilvipalvelumallilla ei olisi toimintaedellytyksiä. Virtualisoinin tarkoitus on piilottaa fyysinen palvelinlaitteisto järjestelmältä, sovelluksilta ja loppukäyttäjältä. Tämä mahdollistaa yhden fyysisen resurssin esittämisen useampana loogisena resurssina. Esimerkiksi yksi fyysinen kiintolevy voi toimia useampana loogisena tallennuslaitteena. Virtualisoinnilla voidaan myös esittää monta fyysistä resurssia yhtenä loogisena resurssina. Pilvipalvelinten virtualisoinnilla parannetaan ohjelmistojen ja laitteiston käyttöönottonopeutta, käyttöastetta, virrankulutusta sekä ongelmatilanteista toipumista. Hyödyt jäävät lähinnä palveluntarjoajalle, mutta näkyvät asiakkaille halvempina hintoina. Heikkoutena voidaan pitää virtualisoinnin tuomaa lisäkerrosta arkkitehtuuriin. Arkkitehtuurin monimutkaistuminen on haitaksi tietoturvalle ja virtualisointiin tarvittavista ohjelmistoista aiheutuu lisäkustannuksia kaupallisille ratkaisuille. (Salo 2010,47–48)

Fyysinen palvelin voidaan jakaa virtualisoinnilla moneen instanssiin. Jokainen instanssi näyttää käyttäjän näkökulmasta kokonaiselta palvelimelta. Sen sijaan, että asiakkaiden tarvitsisi luoda virtuaaliympäristö tyhjästä, pilvipalveluiden tarjoajat tarjoavat instansseihin valmiiksi konfiguroituja käyttöjärjestelmiä. Amazon kutsuu omia hieman käyttöjärjestelmälevykuvia (system image) muistuttavia ”kehyksiä” nimellä AMI (Amazon Machine Image) (kuva 1). AMIsta voidaan käynnistää haluttu määrä instansseja eli virtuaalikoneita kyseisen levykuvan mukaisella käyttöjärjestelmällä. Amazonin IaaS-palveluihin on tarjolla eri käyttöjärjestelmiä useilla eri ohjelmistokokoonpanoilla, joita käyttäjät voivat tehdä ja jakaa muille. (Amazon Web Services 2013)



KUVA 1. Tyypillinen virtualisointi verrattuna Amazonin ratkaisuun (Salo 2010, 48).

Vuoden 2013 alussa haastateltu VMwaren toimitusjohtaja Pat Gelsinger kertoi, että kaikesta maailman palvelinkuormasta 50 - 60 % on virtualisoitua, ja että ajan myötä jopa 90 % kaikesta palvelimista olisi virtualisoitu (Kerner 2013). Tällä hetkellä EMC:n VMware on ylivoimaisesti käytetyin x86-pohjaisten palvelimien virtualisoinnissa, noin 65 %:n markkinaosuudella. Seuraavaksi käytetyimpiä ovat Microsoftin Hyper-V ja Citrixin Xen. (Clabby 2012)

6 PILVIPALVELUIDEN HYÖDYT JA RISKIT

6.1 Hyödyt

Pilvipalveluiden joustavuus tulee kyvystä ottaa käyttöön ja poistaa käytöstä resursseja ilman viivettä muuttuvan tarpeen mukaan, niin että siitä ei aiheudu lisäkustannuksia. Käytön mukaan skaalaus on parhaimmillaan automatisoituna. Ennakoitavissa olevia resurssipiikkejä ovat esimerkiksi mainoskampanjat ja sesongit. Ennakoimattomia piikkejä aiheutuu mm. markkinoiden yllättävistä tapahtumista tai kilpailijoin toimista. Pilvipalveluiden laskutustavasta johtuen yhden prosessorin käyttäminen 100 tunnin ajan kustantaa saman verran kuin 100 prosessorin käyttö tunnin ajan. Rinnakkaislaskennalla voidaan viikkojen mittainen tehtävä suorittaa kustannustehokkaasti muutamassa tunnissa. Pilvipalvelut eivät vaikuta pelkästään tietotekniikkakapasiteetin joustoon, vaan myös sovellusten käyttöönotto. Esimerkiksi Capgemini nopeutti asiakkaidensa kanssa tehdyissä pilottiprojekteissa uusien sovellusten käyttöönottoaikaa parhaimmillaan 70 %. (Salo 2010, 45, 83)

Yllättävien irtisanomisien tullessa yritykselle ei jää lukuisia ylimääräisiä ohjelmalisenssejä, vaan SaaS-palveluista voidaan luopua heti. Yrityksen kasvaessa uusille työntekijöille voidaan tarjota työvälineet jo ensimmäisen työpäivän aikana ilman hankintapäätöksiä tai asennuksia. Palveluiden käyttöönottamisesta on pyritty tekemään mahdollisimman yksinkertaista. Tarpeettomat henkilöiden väliset vuorovaikutukset on pyritty karsimaan itsepalveluilla ja automatisoinnilla. (Salo 2010, 45, 81)

Pilvipalveluiden käyttö vähentää paikkariippuvuutta. Usein mikä tahansa verkkoyhteyden ja verkkoselaimen omaava päätelaite mahdollistaa palveluun pääsyn paikasta riippumatta. Koska laskenta tapahtuu pääosin pilvipalvelimella, on kevyilläkin päätelaitteilla mahdollista käyttää hyvin laskentaintensiivisiä sovelluksia. Tavallisen pöytäkoneen sijasta voidaan käyttää kevyitä asiakaspäätteitä (eng. thin client), jotka ovat suunniteltu vain verkkoselaimen ajoon. Lähivuosina uutena ovat myös tulleet älypuhelimille ja tableteille tehdyt sovellukset, kuten esimerkiksi AWS Console –sovellus iOSille ja androidille, jolla on mahdollista kontrolloida Amazon instansseja. Myös Google on tuonut oman Drive-pilvipalvelunsa yleisimmille mobiilialustoille.

Pilvipalveluihin siirtyminen tarkoittaa resurssien oman hallinnan osittaista menetystä. Useilla yrityksillä on kuitenkin vielä käytössä vanhoja tai tietoturvattomia ratkaisuja, joista on hankalaa ja kallista päästä eroon. Ohjelmistot jäävät monesti päivittämättä jonkin ongelman tai laiskuuden takia. Koneille asennetut selaimet saattavat esimerkiksi olla vanhentuneita versiota vain sen takia, että jokin organisaation käyttämä palvelu kuten intranet ei tue uudempaa versiota. Kova kilpailu asiakkaista motivoi palveluntarjoajat pitämään huolen, että tarjolla olevien palveluiden päivitykset ja tietoturva ovat ajan tasalla. (Salo 2010, 82)

6.2 Riskit

Yksityiseen ja hybridipilveen verrattuna ulkoisissa pilvipalveluissa turvallisuusriskit ovat suurimmat. ICT-alan konsultointi- ja tutkimusyritys Gartner on koonnut seitsemän riskiä, jotka pilvipalveluita harkitsevien tai käyttävien yritysten tulisi huomioida:

1. Ulkopuolisien pääsy tietoihin

   Palveluntarjoajan työntekijöillä ja mahdollisilla kumppaneilla on pääsy laitteistoon ja tietoliikenteeseen, mistä aiheutuu riski tietoturvalle. Myös yrityksen oma henkilöstö voi olla uhka tietoturvalle tietoisesti tai tiedostamatta. Työntekijä voi tahallaan tehdä väärinkäytöksen tavoitellessaan omaa etua. Lisäksi huolimattomuus ja tietämättömyys aiheuttavat merkittävän uhan tietoturvalle. Esimerkiksi jos käyttäjien annettaan päättää omat salasanat, pitää huolehtia, että käytettävät salasanat eivät ole samoja kuin muissa palveluissa tai helposti arvattavia. (Salo 2010, 104) Pienissä ja keskisuurissa yrityksissä 80 prosenttia tietoturvan taloudellisista vahingoista johtuu oman henkilökunnan tahattomista virheistä (Perkiö 2009).

2. Vastuu tallennetusta datasta

   Vaikka data sijaitsee fyysisesti palveluntarjoajan tiloissa, on yrityksen vastuu huolehtia sen säilytyksen turvallisuudesta ja luotettavuudesta. Palveluntarjoajan tiloihin ei välttämättä ole pääsyä, eikä datan tarkkaa säilytys sijaintia ja turvallisuutta ole mahdollista selvittää. (Salo 2010, 105)

3. Tallennetun datan sijainti

   Toimialan luonteesta johtuen palveluntarjoaja ei välttämättä voi edes paljastaa asiakkaille missä maassa dataa säilytetään. Tietosuojalaissa ja muissa IT-alaan vaikuttavissa sääntelyissä on maakohtaisia eroavaisuuksia, jotka pitäisivät huomioida. (Salo 2010, 105)

4. Datan erottaminen muiden asiakkaiden datasta

   Pilvipalveluntarjoajan täytyy pystyä eristämään asiakkaat niin, että heillä ei ole mahdollisuutta nähdä tai vaikuttaa toistensa tietoliikenteeseen ja tallentamiin tietoihin. Kryptaus on eristämiseen tehokas tapa, mutta se ei poista kaikkia ongelmia. Pilvipalveluntarjoajan pitäisi pystyä todistamaan, että heillä käytössä olevat kryptausjärjestelmät ovat kokeneiden asiantuntijoiden suunnittelemia ja testaamia. (Brodkin 2008)

5. Ongelmista toipuminen

   Vaikka datan tallennus sijaintia ei kerrottaisi, palveluntarjoajan pitäisi ilmoittaa mitä tallenteille tapahtuu odottamattoman ongelman tapahtuessa. Jos kaikki data ja sen varmuuskopiot sijaitsevat yhdessä maantieteellisessä sijainnissa, ovat tallennetut tiedot herkempiä niiden täydelliselle menetykselle. Yrityksen on hyvä ottaa selvää kuinka palveluntarjoaja pystyy palauttamaan ongelmatilasta, kauanko palautuminen kestää ja kuinka asiasta informoidaan. (Brodkin 2008)

6. Tutkinnan suorittaminen

   Sopimattomien tai laittomien toimien tutkinta voi olla pilvipalvelussa mahdotonta. Asiaakaan pitäisi olla tietoinen palveluntarjoajan kyvystä toimia tällaisessa tilanteessa. Pilvipalveluita on erityisen vaikea tutkia useiden data kopioiden ja sovellusten alati vaihtaessa paikkaa. (Salo 2010, 105; Brodkin 2008)

7. Palvelun elinkelpoisuus ja jatkuvuus

   Pilvipalveluntarjoajia on markkinoilla lukuisia, mutta osa tulee ajan myötä putoamaan pois. Suurien palveluntarjoajien, kuten Microsoftin, Googlen ja Amazonin voidaan olettaa kestävän pidemmälle tulevaisuuteen mahdollisista vastoinkäymisistä huolimatta. (Salo 2010, 105) Jos palveluntarjoajan palvelut eivät ole standardoitu, voi uudelle palveluntarjoajalle siirtyminen olla hyvin työlästä.

> Jopa tallennustilaa tarjoava palvelu saattaa olla epäyhteensopiva toisen palveluntarjoajan vastaavanlaisen palvelun kanssa. Joidenkin yritysten tiedetään luovan tahallaan vaikeasti irtipäästäviä palveluita. Esimerkiksi Amazonin S3 (Simple Storage Service) ei ole yhteensopiva IBM:n, Googlen tai Dellin luomien ratkaisujen kanssa. (Rong, Nguyen & Jaatun, 4)

6.3 Palvelun saatavuus

Monelle yrityksellä on kriittistä, että palvelut ovat aina saatavilla. Palveluntarjoajat tarjoavat sopimuksia, joilla pyritään vakuuttamaan asiakkaalle palvelun luotettavuus. Palvelutasosopimus (SLA, Service Level Agreement) ja laatulupaus (QoS, Quality of Service) ovat tärkeitä kun suunnitellaan siirtymistä ulkoisen palveluntarjoajan palveluihin. Palvelutasosopimuksessa palveluntarjoaja sitoutuu pitämään palvelutason luvatun rajan yläpuolella huoltokatkoksista ja vikatilanteista riippumatta. Sopimuksessa myös käydään läpi asiakkaan saamat hyvitykset, jos luvattuihin palvelutasoihin ei päästä. (Salo 2010, 112) Hyvitykset ovat tyypillisesti alennuksia tai hyvityslaskuja. Palvelun saatavuus (uptime) eli palvelutaso ilmoitetaan prosentteina (taulukko 1). Luvatut palvelutasot ovat tyypillisesti hyvin lähellä 100 prosenttia.

TAULUKKO 1. Saatavuudet luvatulla palvelutasolla eri aikajaksoilla (Salo 2010, 112).

	Palvelutaso (SLA) lukuina		
Palvelutaso	Palvelu poissa käytöstä / vuosi	Palvelu poissa käytöstä / kuukausi	Palvelu poissa käytöstä / päivä
100,00 %	0 h 0 min	0 h 0 min	0 min 0
99,99 %	0 h 53 min	0 h 4 min	0 min 8,8
99,95 %	4 h 38 min	0 h 22 min	0 min 43,8
99,90 %	8 h 46 min	0 h 44 min	1 min 27,6
99,00 %	87 h 36 min	7 h 18 min	14 min 36,0

Palvelinklusteri on tehokas ratkaisu katkoksien välttämiseen. Klusterissa joukko tietokoneita on verkotettu yhteen niin, että ne toimivat yhtenä kokonaisuutena. Asiakkaan virtualisoitu palvelinympäristö on sijoitettuna palvelinklusteriin, joka koostuu ainakin

kahdesta fyysisestä palvelinlaitteesta. Jos fyysinen palvelin vikaantuu, asiakkaan palvelut siirtyvät automaattisesti toisen palvelimen varaan alle minuutissa. Fyysisille palvelimille tehtävien huoltotöiden, kuten päivityksien ajaksi asiakkaan palvelin siirretään toiselle laiteella käyttäjän sitä huomaamatta. (Vikasietoiset palvelut 2013)

6.4 Vinkkejä pilvipalveluihin siirtymistä harkitseville yrityksille

Julkisten pilvipalveluiden katsotaan soveltuvan parhaiten etenkin uusille tai pienille yrityksille, joille riittää valmiit kustomoimattomat ohjelmistot. Varta vasten yritykselle luotuja ohjelmistoja saattaa olla mahdoton toi hyvin hankala siirtää pilveen. Pilvi auttaa erityisesti pienyrityksiä vastaamaan nopeammin ja tehokkaammin asiakkaiden tarpeisiin. Mielessä kannattaa pitää myös, ettei kaikkia IT-resursseja tarvitse eikä välttämättä kannata siirtää pilveen.

Seuraavien kohtien pitäessä paikkaansa tulisi yrityksen harkita pilvipalveluihin siirtymistä. Jos

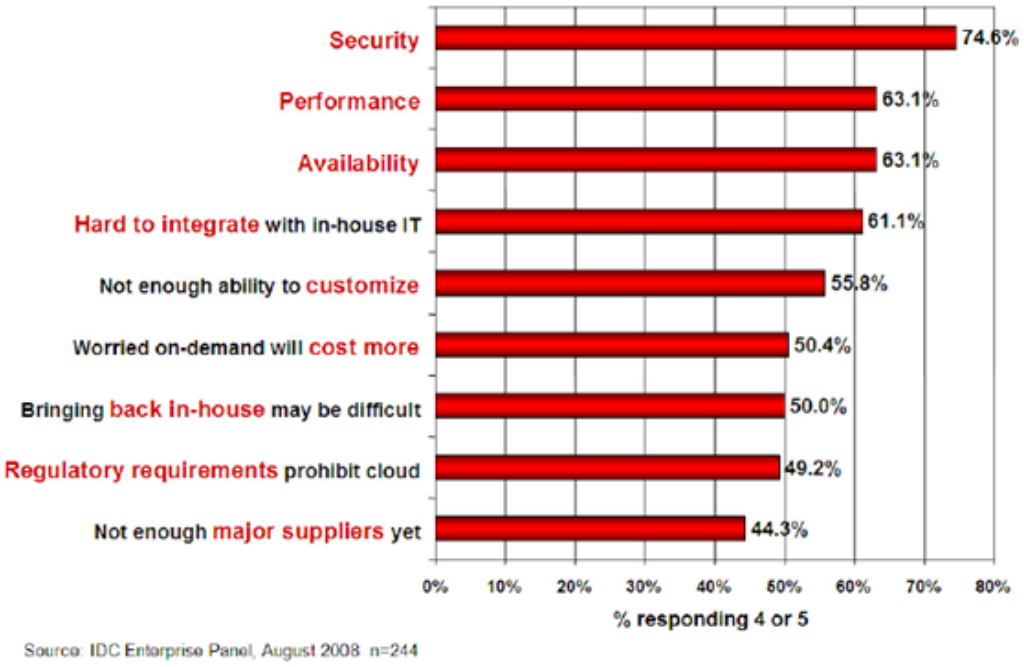
- yrityksen tarvitsee tehdä suuria leikkauksia IT-kuluihin
- tietoihin pitää päästä käsiksi myös toimitilojen ulkopuolelta
- yritys tulee toimeen ilman kustomoituja ja yksinoikeudella valmistettuja sovelluksia.
- kilpailijat ovat suuria yrityksiä
- IT-resurssien tarve on vaihtelee suuresti (skaalautuvuus)
- yksikään käytössä olevat sovellukset ovat elinkaarensa päässä
- palvelinlaitteisto on yli 5 vuotta vanhaa
- yritys tarvitsee paremman toipumissuunnitelman. (Sippola 2012)

Palveluntarjoajaa valittaessa tulisi selvittää kuin palveluista pääsee tarvittaessa eroon ja onko vaihto toiseen mahdollista ongelmitta. Palvelun tarjoajien SLA-sopimuksia on myös hyvä vertailla.

7 PILVIPALVELUIDEN TIETOTURVA

7.1 Tietoturva yleisesti

Pilvipalveluiden hurjassa kehityksessä on myös haittapuolensa, jatkuvasti uudistuvia palveluita on vaikea keritä hiomaan turvallisiksi, kun palvelut jo taas muuttuvat ja uusia tietoturva-aukkoja ilmenee. Yrityksen tietoturvan pitääkin siis olla aina ajan tasalla eikä sitä voi missään vaiheessa jättää laakereille lepäämään. Yhä useammat yritykset ovat kiinnostuneet pilvipalveluista, mutta heillä ei ole varaa riskeerata yrityksen ohjelmistojen ja datan tietoturvaa. IDC:n tekemän tutkimukseen vastanneiden IT-johtajien ja tietohallintopäälliköiden mielestä tietoturva on pilvipalveluiden suurin ongelma (kuva 2).



KUVA 2. Vastukset kyselyyn pilvipalveluiden ongelmista (Cloud Computing – Relevance to Enterprise 2011).

Enemmistö tietoturvauhkatilanteista aiheutuu vain huolimattomuuden tai tietämättömyyden takia, kuten seuraavassa esimerkissä: saksalaisessa Darmstadtin tutkimuskeskuksessa huomattiin Amazonin käyttäjien jakamien AMI-järjestelmälevykuvien olevan suuri tietoturvariski jakoon laittaneelle organisaatiolle. Tutkimuksiin otettiin mukaan 1100 yleisessä jaossa olevaa AMIa, joista 30 %:sta löytyi tarpeeksi tietoja, jotta tekijän

pilvipalveluresurssit olisi voitu ottaa osittain tai kokonaan haltuun. Tutkijoiden mukaan AMIt sisälsivät tekijöiden yksityisiä salausavaimia, salasanoja ja varmenteita, esimerkiksi komentohistorian poistamatta jättämisen vuoksi. Amazon on ollut pitkään tietoinen potentiaalisesta tietouhasta ja julkaissut ohjeita AMIen turvallisempaan jakamiseen. (Walker-Morgan 2011)

7.2 Tietoturvauhat

Pilvipalveluiden tietoturvan parantamiseen on keksitty lukuisia standardeja ja asetuksia, mutta voittoa tavoittelematon Cloud Security Alliance (CSA) on pyrkinyt tarjoamaan koko pilvipalvelumarkkinoita kattavan tietoturvasertifikaatin. CSA on tietoturva ja pilviasiantuntijoiden johtama organisaatio, jonka jäseniä ovat mm. Google, Microsoft, VMware ja IBM. (Salo 2010, 106) Helmikuussa 2013 CSA julkaisi päivitetyn version ”Top Threats to Cloud Computing” –raportista. Raportissa on listattuna pilvipalveluiden tämän hetken suurimmat tietoturvauhat palveluiden ylläpitäjien ja käyttäjien kannalta. Seuraavissa välikappaleissa käydään läpi listalta löytyvät uhat ja joitakin esimerkki tapauksia.

7.2.1 Tietomurrot

Pelko siitä, että organisaation arkaluonteiset tiedot pääsevät vääriin käsiin, on ollut olemassa jo kauan ennen tietotekniikkaa, pilvipalvelut tuovat kuitenkin mukanaan huomattavan määrän uusia keinoja hyökkääjille. Jos palveluntarjoajan palveluita ei ole suunniteltu oikein monikäyttäjyyttä ajatellen, vika yhden asiakkaan ohjelmassa voi avata tietoturva-aukon muidenkin käyttäjien tietoihin. Suuret käyttäjämäärät tekevät pilvipalveluista houkuttelevia kohteita verkkovandaaleille ja yrityssalaisuuksia havitteleville tahoille. (Cloud Computing Top Threats in 2013, 8; Salo 2010, 110)

Marraskuussa 2012 julkaistiin tietoturvayritys RSA:n ja Amerikkalaisten yliopistojen yhteistyönä tehdyn tutkimuksen raportti, jossa selvitettiin kuinka pilven virtuaalikone voisi käyttää sivukanavien ajoitustietoa (side channel timing information) ja purkaa toisen samalla fyysisellä palvelimella pyörivän virtuaalikoneen salausavaimen. (Cloud Computing Top Threats in 2013, 8)

Yksi tapa tietomurtoja vastaan on tietojen salaaminen. Vaikka palveluntarjoajan turvakeinot pettäisivät, estäisi riittävä salaus luvattoman pääsyn tietoihin. Kaikki pilvipalvelut eivät kuitenkaan tue salausta, ja salausavaimen hukkuessa, menetetään myös salattu tieto. Vaihtoehtoisesti organisaatio voi pitää offline-varmuustallenteita, välttääkseen tietojen totaalisen menettämisen, mutta samalla tämä lisää altistumista tietomurroille. (Cloud Computing Top Threats in 2013, 8)

7.2.2 Tietojen menetys

Pilveen tallennetut tiedot voivat hävitä haitallisten hyökkäysten lisäksi palveluntarjoajan virheestä johtuen tai fyysisten katastrofien, kuten tulipalon tai maanjäristyksen aiheuttamana, ellei riittäviä varmuuskopiota oteta. Monet palveluntarjoajat, kuten Microsoft ja Amazon, varmistavat tietojen säilymisen tallentamalla ne kolminkertaisesti (Salo 2010, 110). Säilyttämisen lisäksi palveluntarjoajan pitää huolehtia, että asiakkaan halutessa poistaa tietoja, ne hävitetään lopullisesti.

Tietoa voidaan tuhoutumisen lisäksi menettää korruptoitumisen seurauksena. Jotkut tallennustilapalvelut kuten Amazonin S3 sisältävät valmiit toiminnot tarkistussumman (checksum) tai tiivisteen (hash) tarkastamiseen. Tiiviste on alkuperäisen informaation hyvin pieneksi tiivistetty muoto, jota voidaan käyttää informaatioiden vertailuun, mutta ei palautukseen. S3 tukee esimerkiksi MD5-tiivisteitä, joiden avulla voidaan varmistaa, että siirretty tai varastoitu tieto on säilynyt muuttumattomana (Rittinghouse & Ransome 2010, 171).

EU:n uusien tietosuojasääntöjen mukaan asiakkaan henkilötietojen tuhoutuminen tai korruptoituminen lasketaan tietyn tyyppiseksi tietomurroksi ja edellyttää täten asianmukaisen ilmoituksen. (Cloud Computing Top Threats in 2013, 9)

7.2.3 Käyttäjätilin tai palvelun liikenteen kaappaaminen

Käyttäjätilien ja palveluiden liikenteen kaappaaminen ei ole uutta. Tietojenkalastelulla, petoksilla ja ohjelmistohaavoittuvuuksien hyväksikäytöllä saavutetaan kuitenkin edelleen tuloksia. Samojen valtuustietojen (credentials) ja salasanojen uudelleen käyttö edesauttaa tunnusten kaappauksia. Jos hyökkääjä saa haltuunsa valtuustiedot, voi hän seurata tapahtumia ja liiketoimia, manipuloida tietoja, palauttaa väärennettyjä tietoja ja ohjata yrityksen asiakkaita väärille sivuille. Vallatusta instanssista tai tunnuksesta voi tulla uusi väline seuraavaan tietoturvahyökkäykseen. (Cloud Computing Top Threats in 2013, 10)

Huhtikuussa 2010 hyökkääjät löysivät Amazon Wireless -sivustolta haavoittuvuuden, joka mahdollisti sivustojen välisen komentosarjahyökkäyksen (Cross-Site Scripting, XSS). Hyökkäyksellä kaappaajat saivat ryöstettyä sivuille kirjautuneiden käyttäjien valtuustietoja. (Goodin 2010)

Kaikki arkaluonteiset asiat pilvessä olisi turvallisinta hoitaa salatuilla yhteyksillä. SSL-salausta (Secure Sockets Layer protocol) käyttämällä internetin yli kulkeva liikenne voidaan salata molempaan suuntaan. Jos pilvipalvelun tiedonsiirrossa käytetään salausta, yrityksen pitäisi pyrkiä kontrolloimaan salaukseen käytettäviä avaimia. (Rittinghouse & Ransome 2010, 158)

Kaappauksien estämiseksi organisaation pitäisi kieltää valtuustietojen jakaminen käyttäjien ja palveluiden välillä sekä, jos mahdollista, hyödyntää kahden tekijän todennusta (two-factor authentication), jossa esimerkiksi sisäänkirjautuessa salasanan lisäksi tarvitaan tekstiviestillä vastaanotettava koodi. (Cloud Computing Top Threats in 2013, 10) Käyttämällä ennakoivia järjestelmän monitorointisovelluksia, voidaan luvattomat toiminnat havaita, ennen suurempia vahinkoja. Pilvipalveluita käyttävien henkilöiden olisi myös hyvä perehtyä palveluntarjoajan tietoturvaohjeisiin ja SLA-sopimukseen. (Top Threats to Cloud Computing V1.0 2010, 13)

7.2.4 Turvattomat rajapinnat

Pilvipalveluntarjoajat antavat käyttäjille rajapintoja (API) pilvipalveluiden resurssien hallintaan, organisointiin ja monitorointiin. Rajapintojen avulla käyttäjien sovellukset voivat olla vuorovaikutuksessa palveluntarjoajan toiminnallisuuksiin. Usein koko pilvipalvelun turvallisuus ja saatavuus riippuvat rajapintojen tietoturvasta. Rajapinnat pitää olla suunniteltuna niin, että ne ovat suojassa haitallisilta toimilta ja käyttäjien vahingoilta. Pilvipalveluita käyttävät yritykset saattavat tarjoavat omille asiakkailleen palveluita, jotka vaativat rajapintoja myös kolmansilta osapuolilta. Uusi rajapintataso tuo järjestelmään monimutkaisuutta, joka lisää tietoturvariskiä. Riski syntyy, jos yrityksen täytyy luovuttaa valtuustietoja kolmannelle osapuolelle API-toimintojen mahdollistamiseksi. (Cloud Computing Top Threats in 2013, 12)

Cloud Security Alliance neuvoo analysoimaan palveluntarjoajan rajapintojen tietoturvamallia sekä varmistamaan, että käytössä olevat autentikointi- ja pääsynvalvontatiedot toteutetaan salattuna. Käyttäjillä pitäisi olla hyvä käsitys rajapintojen riippuvuuksista ja vaikutuksista tietoturvaan. (Top Threats to Cloud Computing V1.0 2010, 9)

7.2.5 Palvelunestohyökkäykset

Palvelunestohyökkäyksessä (Denial of Service, DoS) käyttäjän palvelu lamautetaan niin, että sen käyttö häiriintyy tai estyy kokonaan. Hyökkäyksellä ei siis varsinaisesti pyritä varastamaan mitään. Pilvipalvelua vastaan tehty palvelunestohyökkäys pakottaa uhrin pilvipalvelun kuluttamaan suuren määrän järjestelmäresursseja, kuten laskentatehoa, muistia, tallennustilaa tai verkon kaistaa. Hyökkääjä tai hyökkääjät, jos kyseessä on hajautettu palvelunestohyökkäys (DDoS), voivat hidastaa palvelun tai täyttää järjestelmän tallennuskapasiteetit käyttökelvottomiksi. Kaiken lisäksi pilven käyttökustannukset saattavat nousta hyökkäyksen ajaksi hyvin kalliiksi, jolloin ainoaksi vaihtoehdoksi jää palveluiden alas ajaminen. (Cloud Computing Top Threats in 2013, 14) Pahimmassa tapauksessa pilvipalvelun käyttäjä ei pysty hyökkäyksen takia edes hallitsemaan pilveä.

Palvelunestohyökkäyksiä vastaan on hyvin vaikea puolustautua. Hyökkäyksien varalle olisi hyvä olla monitorointi sovellus, joka varoittaisi alkaneesta hyökkäyksestä mahdollisimman nopeasti. Monitorointi voidaan toteuttaa yksinkertaisella skriptillä, joka lähet-

tää viestin pilvipalvelimelta tietyin väliajoin ja hälyttää, jos välit kasvavat liian suuriksi tai viestiä ei saavu ollenkaan. Hajautetussa palvelunestohyökkäyksessä hyökkääjien IP-osoitteiden estäminen on lähes mahdotonta. DDoS-hyökkäys perustuu raakaan voimaan, joten hyökkääjillä pitää kuitenkin olla yksilöllisiä yhtäläisyyksiä. Yhtäläisyys on usein saapuvien pakettien URI-, user agent- tai referer-tiedoissa. Jos käyttäjällä on mahdollisuus muokata esim. pääsyvalvontalistaan tai palomuurin suodatuksia, on hyökkääjien liikenteen sisäänpääsy mahdollista estää. Menettely ei kuitenkaan poista palveluun saapuvan liikenteen hidastumista, mutta vapauttaa pilven muita resursseja taakasta. Pilvipalveluita vastaan tehtyjä DDoS-hyökkäyksiä on lähes mahdoton torjua täysin, mutta torjunnan avuksi on olemassa maksullisia palveluita ja ohjelmistoja, joilla vahinko voidaan minimoida. (Five Ways to Protect Against DDoS Attacks 2013)

7.2.6 Palveluntarjoajan työntekijät

Virheellisesti suunnitellussa pilvijärjestelmässä mahdollisesti epäluotettava henkilö, kuten pilvipalvelun järjestelmänvalvoja pääsee käsiksi asiakkaan arkaluonteisiin tietoihin. IaaS:ää voidaan pitää tässä tietoturvamielessä PaaS:ää ja SaaS:ää turvallisempana. Mitä suuremman osan tietoturvasta pilvipalveluntarjoaja hoitaa, sitä kriittisempiin järjestelmiin ja tietoihin palveluntarjoajalla on pääsy. Vaikka järjestelmän voisi salata, jos salausavaimet eivät ole käyttäjän hallussa ja ovat käytössä vain datan käytön ajan, järjestelmä on edelleen haavoittuvainen haitallisille sisäpiirihyökkäyksille. (Cloud Computing Top Threats in 2013, 16) Jos palvelu mahdollistaa luotettavan monitoroinnin, tapahtumia olisi hyvä seurata tietokannan toiminnan valvontaohjelmalla.

Myös vahinkoja sattuu, esimerkiksi vuoden 2012 jouluaattona Amazonin Web Services-pilvessä pyörinyt videoiden streamaus palvelun Netflixin palvelut lakkasit osittain toimimasta. Lähes vuorokauden pysähdys tapahtui kun Amazonin työntekijä poisti vahingossa tärkeää dataa huoltotöiden yhteydessä. (Musil 2012)

7.2.7 Pilvipalveluiden väärinkäyttö

IaaS- ja PaaS-palveluiden tuoma vapaus houkuttelee myös pilvipalvelun väärinkäyttäjiä ja rikollisia. Pääsy valtaviin laiteresursseihin ei vaadi kuin luottokortin ja rekisteröinnin

jälkeen palvelu on heti käytettävissä. Jotkut palveluntarjoajat antavat jopa ilmaisia kokeiluaikoja. Hyödyntämällä palvelun lähes anonyymisti tehtävää käyttöönottoa, voivat väärinkäyttäjät suorittaa palvelulla haitallista koodia, esimerkiksi roskapostin lähetykseen tai bottiverkon ohjaukseen. Huolenaiheena on, että tulevaisuudessa pilvipalveluiden laskentatehoa käytetään salauksien ja salasanojen purkamiseen, sateenkaaritaulujen rakentamiseen sekä CAPTCHA-kuvavarmennusten ratkaisemiseen. (Top Threats to Cloud Computing V1.0 2010, 8)

Laillisten ja laittomien asiakkaiden erottelu on pilvipalveluntarjoajille ongelma, palveluiden rankan automatisoinnin takia. Pilvipalveluiden väärinkäyttö aiheuttaa ongelmia lähinnä palveluntarjoajille itselleen. Vaarana on kuitenkin, että organisaation käytössä olevat IP-osoitteet joutuvat mustalle listalle. Roskapostia lähettävät tahot käyttävät dynaamisia IP-osoitteita, jotka voivat vaihtua hetkessä toiseen. Yhden IP-osoitteen estäminen ei ole siis tarpeeksi, vaan mustille listoille voi joutua suuria osoiteavaruuksia, joista osa kuuluu luotettaville organisaatiolle. Asiakkaiden pitäisi siis monitoroida julkisia mustia listoja, omia IP-osoitteita silmällä pitäen. (Krebs 2008)

On hyvä huomioida, että julkisessa pilvessä resurssit jaetaan muiden asiakkaiden kanssa, ja jos joku asiakkaista jää kiinni laittomista toimista, voi tapahtua tilanne, jossa yrityksen pilviresurssit takavarikoidaan valtion toimesta vain siksi, että yritys ja rikollinen käyttivät samaa ympäristöä pilvessä. (Rittinghouse & Ransome 2010, 158)

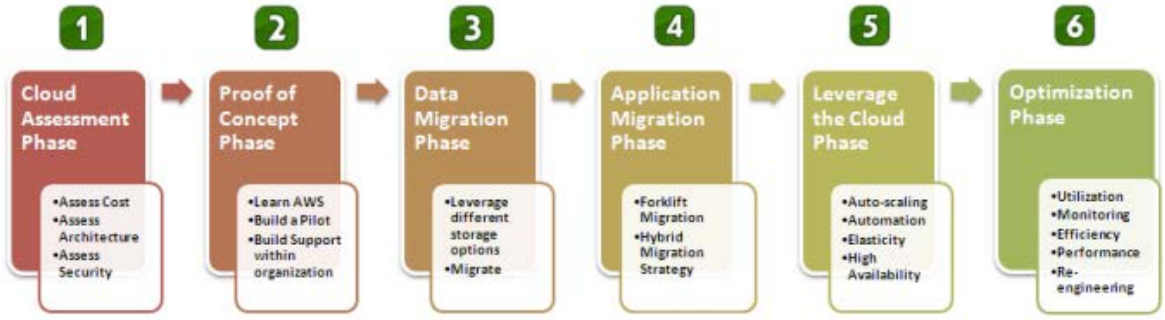
7.2.8 Tunnistamattomat riskit

IT-infrastruktuurin ulkoistaminen pilveen saattaa tuntua ideana hyvältä, mutta ennen muutosta organisaatiolla pitäisi tiedostaa kaikki pilven mukana tulevat tietoturvariskit. Pilvipalvelun tuomia laitteisto-, ohjelmisto- ja ylläpitosäästöjä olisi hyvä verrata uusiin tietoturvariskeihin. Palveluntarjoajat eivät monesti kuitenkaan tarjoa palveluistaan riittävästi tietoa asiakkaille. Puutteelliset tiedot asioista, kuten käyttäjien datan sijainnista, kuinka palveluita käytetään turvallisesti ja mitä riskejä palvelun käyttöön saattaa liittyä. (Top Threats to Cloud Computing V1.0 2010, 14)

Käytössä olevat ohjelmistot saattavat olla riippuvaisia organisaation sisäisen verkon tietoturvan hallinnasta, joten niiden siirto pilveen voi olla vaarallista järjestelmän liian

vähäisen kontrollin takia. Tuntemattomia toiminta- ja arkkitehtuuriongelmia saattaa ilmetä, kun aletaan suunnitella ohjelmia vieraaseen pilvitekniikkaan. (Cloud Computing Top Threats in 2013, 19) Uusien työntekijöiden tai konsulttien palkkaaminen voi olla edessä, jos IT-väeltä puuttuu kokemusta pilvipalveluympäristöistä.

Siirtyminen perinteisestä palvelinympäristöstä pilveen ei ole helppoa, mutta ongelmat ovat harvoin palveluntarjoajan päästä. Organisaation pitää pystyä tekemään pilveen siirtymisestä selkeä muuttosuunnitelma. (Perfecting the Unknown: Cloud Computing 2012) Suunnitelman tekoon löytyy verkosta useita kattavia ohjeita. Kuvan 3 esimerkki antaa osviittaa muuton vaiheista.



KUVA 3. Esimerkki muuttosuunnitelman vaiheista (Rae 2011).

Jos siirtyminen pilveen on jo tehty, on organisaation tietoturvallisuus hyvä kartoittaa. Turvallisuuden kartoittamisessa yritys voi käyttää hyväkseen alan asiantuntijoiden luomia ohjeita tai luottaa omaan osaamiseensa. Esimerkiksi pienille ja keskisuurille yrityksille on ilmaiseksi tarjolla Tieken (Tietoyhteiskunnan kehittämiskeskus ry) tietoturvakartoituskysely. Suuremmille yrityksille suositellaan Jericho Forumin erityisesti pilvipalvuiden tietoturvaa varten tehtyä kartoituskyselyä SAS (Self-Assessment Scheme). (Salo 2010, 106)

7.2.9 Jaetun teknologian haavoittuvuudet

Pilvipalvelutarjoajien palvelut perustuvat skaalattaviin infrastruktuureihin, alustoihin ja sovelluksiin. Valitettavasti palveluita ylläpitävä laitteisto ei aina ole suunniteltu monikäyttäjyyttä ajatellen. Esimerkiksi tehtävään sopimaton CPU:n välimuisti tai GPU voi aiheuttaa tietoturva-aukon käyttäjien välille pilvipalvelumallista riippumatta. Yksikin

haavoittuvuus tai virheellinen konfigurointi hypervisorissa (IaaS), jaetussa alustassa (PaaS) tai SaaS-ympäristön ohjelmassa voi vaarantaa koko palvelutarjoajan pilven. (Cloud Computing Top Threats in 2013, 21)

Hypervisoriksi kutsutaan valvontaohjelmistoa, joka hoitaa fyysisten palvelinresurssien jaon virtuaalikoneille. Pilviympäristössä sen yksi tarkoitus on pitää virtuaalikoneet eristettynä toisistaan niin, että mitkään asiakkaiden tekemät toiminnat ei näy tai vaikuta muiden asiakkaiden virtuaalikoneisiin. Silloin tällöin kuitenkin paljastuu uusia tietoturva-aukkoja, joiden avulla virtuaalikoneiden käyttäjä ovat pystyneet suorittamaan koodia virtuaaliympäristön ulkopuolella.

Viime vuonna keskustelua aiheutti US-CERTin (U.S. Computer Emergency Readiness Team) tietoturvavaroitus koskien Xen-pohjaisia Intelin CPU:lla pyöriviä virtualisointituoteita ja niistä löytynyttä haavoittuvuutta, jonka avulla hyökkääjä pystyi saamaan admin-tason oikeudet ja ajamaan muita vahingoittavaa koodia tai kirjautumaan mille tahansa käyttäjätilille. Kyseistä haavoittuvuuden uhkaa lievensi kuitenkin se, että hyökkääjällä piti olla kelvolliset valtuustiedot ja kirjautuminen oli tehtävä paikallisesti. (Schwartz 2012)

Cloud Security Alliance on listannut muutamia asioita mitä IaaS-palvelussa voidaan tehdä uhan torjumiseksi:

- Monitoroida virtuaalikoneiden toimintaa.
- Haavoittuvuus skannaus ja asetusten tarkastuksia.
- Vahva autentikointimenetelmä ja kulunvalvonta ylläpitotunnuksille.
- Vaatia palvelutasosopimuksessa (SLA) nopeat tietoturvapäivitykset haavoittuvuuksien korjaamiseen. (Top Threats to Cloud Computing V1.0 2010, 11)

7.3 Pilvitekniikan positiiviset vaikutukset tieturvaan

Vaikka edellisissä kappaleissa käytiinkin läpi useita pilvipalvelun mukana tulevia tietoturvariskejä, voi pilveen siirtymisellä silti olla positiivinen vaikutus tietoturvaan perinteisiin ohjelmistoihin ja palvelimiin verrattuna. SaaS-mallissa, jossa palveluntarjoajalle jää hoidettavaksi suurin osa tietoturvasta, pystyy toimittaja keskimäärin parempaan turvatasoon kuin keskivertokäyttäjä. Etenkään pk-yrityksillä ei aina ole resursseja tai

osaamista huolehtia riittävästi tietoturvasta, kun taas palveluntarjoajalla tietoturvasta vastaavat tietoturva-alan ammattilaiset.

Tiedot ovat yleensä sekä tietoturvan että saatavuuden kannalta paremmin tallessa pilvessä kuin käyttäjien päätelaitteilla. Tiedot voidaan menettää kiintolevyn rikkouduttua tai, jos tietokone varastetaan tai hukkuu. Pilvessä taas tallennetut tiedot ovat aina saatavilla ja automaattisesti varmuuskopioituna. (Rinne 2012, 52)

Varoittava esimerkki on vuonna 2010 Ponemon Instituten julkaiseman ja Intelin sponsoroiman tutkimuksen tulos Yhdysvaltalaisten organisaatioiden hukkaamista kannettavista tietokoneista. Tutkimuksessa mukana olleet 329 organisaatiota hukkasivat ja menettivät vuoden aikana 86 455 kannettavaa, joka oli yli 7 prosenttia kaikista kannettavista. Hukatuista ja ryöstetyistä kannettavasta aiheutui organisaatiolle keskimäärin 49 000 dollarin kustannukset. (The Billion Dollar Lost Laptop Problem 2010, 1–2)

7.4 Lait ja sopimukset

Riippuen yrityksen toiminnasta pilvipalvelussa, voi laki edellyttää tiettyjen tietojen suojaamista automaattisesti. Jos yritys päättää esimerkiksi siirtää asiakkaan tietoja pilveen, pitää Suomen henkilötietolaista ottaa huomioon 22 §, jonka mukaan ”Henkilötietoja voidaan siirtää Euroopan unionin jäsenvaltioiden alueen tai Euroopan talousalueen ulkopuolelle ainoastaan, jos kyseisessä maassa taataan tietosuojan riittävä taso.” Siirrettäessä tietoja EU:hun kuuluvaan maahan, noudatetaan samoja lainsäädäntöjä kuin Suomen sisällä tapahtuvissa käsittelyissä. Myös Euroopan talousalueeseen (ETA) kuuluvat Islanti, Norja ja Liechestein katsotaan kuuluvan henkilötietojen siirron osalta samaan kategoriaan kuin muut EU-maat. (Henkilötietojen siirto ulkomaille henkilötietolain mukaan 2010, 3–4) Tiedon varastointitilaa myyvät pilvipalveluntarjoajat tiedostavat ongelman, ja siksi suuret pilvipalvelun tarjoajat, kuten Amazon antavat mahdollisuuden valita, mihin palvelinkeskukseen tallennetut tiedot sijoitetaan.

Vuonna 2000 solmittiin Yhdysvaltojen ja Euroopan unionin välille Safe Harbor -järjestelmä, jolla varmistetaan riittävä tietosuoja henkilötietojen siirrossa Yhdysvaltoihin sijoittuneille organisaatiolle. Yhdysvaltalaiset organisaatiot voivat liittyä Yhdysvaltain kauppaministeriön (US Department of Commerce) ylläpitämälle luettelolle organi-

saatiosta, jotka ovat ilmoittaneet noudattavansa Safe Harbor –periaatteita. Järjestelmään liittyminen on julkista ja täysin vapaaehtoista. Liittyneiden organisaatioiden on noudatettava tietosuojaperiaatteita henkilötietojen suojaamiseksi, tai vastaan voidaan nostaa kanne. (Henkilötietojen siirto ulkomaille henkilötietolain mukaan 2010, 6) Järjestelmän tietosuojaperiaatteet ovat:

- Henkilölle ilmoitettava tarkoitus mihin tietoa kerätään ja käytetään.
- Henkilölle pitää antaa mahdollisuus valita, saako hänen tietojaan luovuttaa kolmansille osapuolille.
- Varmistaa, että jos tiedot luovutetaan kolmannelle osapuolelle, myös tämä noudattaa samaa yksityisyyden suojaa.
- Henkilöllä on oltava pääsy henkilökohtaisiin tietoihin.
- Organisaation on otettava käyttöön tarvittavat toimet suojatakseen tietoja häviämiseltä, väärinkäytöltä ja paljastumiselta.
- Varmistettava tietojen oikeellisuus.
- Oltava käytössä riittävät menettelyt, joilla varmistetaan periaatteiden noudattaminen. (Rittinghouse & Ransome 2010, xxxii-xxxiii)

7.5 Turvastandardit ja -asetukset

Yrityksen toimenkuvasta riippuen yrityksen tulee noudattaa määrättyjä asetuksia ja standardeja. Olisi siis selvitettävä mitkä standardit ja asetukset ovat pakollisia, mitä asiakkaat ja yhteistyökumppanit vaativat, mitä yritys haluaa vapaaehtoisesti noudattaa sekä mitä järjestelmiä nämä standardit ja asetukset koskevat.

Yhdysvalloissa toimivia pörssilistattuja yrityksiä ja niiden ulkomaisia tytäryhtiöitä koskettaa lain määräämä SOX-asetus (Sarbanes-Oxley Act), joka määrittää tiukat säädökset taloudellisien raportointien oikeellisuuden kannalta oleellisille järjestelmille. Jos taas yritys vastaanottaa, tallentaa tai välittää kansainvälisiä maksukorttitapahtumia, vaaditaan yritykseltä PCI DSS –tietoturvastandardin (Payment Card Industry Data Security Standard) noudattamista. Turvastandardeja ja –asetuksia on määrätty myös muille lain näkökulmasta tärkeille aloille, kuten ihmisten henkilökohtaisia terveys- ja pankkitietoja käsitteleville osapuolille. (Salo 2010, 106)

Pilvipalvelumarkkinoiden nuoruus ja hajanaisuus tekevät pilvien tietoturvaongelmien ratkaisemisesta haasteellista. Kolmannen osapuolen yritykset ovat tuoneet omia ratkaisujaan palveluntarjoajien turvallisuusongelmiin. Yksi esimerkki on Novellin Novell Cloud Security Service –tietoturvaratkaisu, jonka mainostetaan selkeyttävän kokonaisuutta, parantavan käyttöoikeuksien hallintaa ja turvallisuutta. Järjestelmä tukee useiden turvastandardien vaatimia ominaisuuksia, kuten tapahtumalokeja ja kertakirjautumista (Single Sign-on, SSO). (Salo 2010, 104)

POHDINTA

Työssä tutustuttiin pilvipalveluihin ja sen eri malleihin sekä läpikäytiin yritysten kannalta oleelliset tietoturvaongelmat pilvessä. Pilvipalveluiden tarjonta on kasvanut hyvin suureksi. Ne eivät kuitenkaan sovellu kaikkien yritysten tarpeisiin. Pilvipalveluihin siirtyminen ei tule ratkaisemaan yrityksen kaikkia ongelmia, vain osan, ja mukana tulee aina väistämättä uusia huolenaiheita. Vaihtokauppa voi kuitenkin olla monelle kaiken kaikkiaan positiivinen, koska ohjelmien asentelu ja päivittäminen sekä monimutkaisen infrastruktuurin ylläpito teettävät valtavasti ylimääräistä työtä yrityksille.

Lähes kaikkia tietoturva uhkia vastaan voidaan ainakin jossain määrin puolustautua tai uhan riskiä vähentää. Pilvipalveluntarjoajalla saattaa olla pilvimallista riippuen hyvinkin suuri vastuu yrityksen tietoturvan osalta, joten sen valinnassa pitäisi olla hyvin tarkka. Etenkin SaaS-palveluissa palveluntarjoajalla on kaikki oikeudet ja täysi kontrolli tietoturvasta, kun taas IaaS-palveluissa asiakas voi itse vaikuttaa tietoturvaan laitteistoa lukuun ottamatta. Valitun palveluntarjoajan kanssa tulisi tehdä mahdollisimman aukoton sopimus mm. sen suhteen mitä tapahtuu, jos palvelun kanssa ilmenee ongelma. Kaikkea tieto ei välttämättä kannata siirtää pilveen, vaan tärkeimmät tiedostot on hyvä säilyttää paikallisesti niin, että niihin pääsevät käsiksi vain välttämättömät henkilöt. Tärkeä osaalue on myös yrityksen omien työntekijöiden tietoisuus tietoturvariskeistä, koska keskimäärin jopa 80 % liiketoiminnan tietoturvallisuudesta riippuu henkilöstön rutiineista. Yrityksen tulisi siis panostaa ensisijaisesti henkilökunnan kouluttamiseen ja muistaa, ettei arkaluonteista tietoa leviä ainoastaan verkon välityksellä, vaan myös fyysisten asiakirjojen ja muistioiden sekä puheen välityksellä.

Idea pilvipalveluista opinnäytetyöaiheena tuli alkujaan koululta. Muutamasta eri aihe vaihtoehdosta päädyin pilvipalveluihin sen ajankohtaisuuden ja aikaisempien kokemuksien vuoksi. Aihe oli jo ennestään jokseenkin tuttu, koska erinäisissä koulutöissä oli tullut käytettyä Amazonin AWS-virtuaalikoneita sekä perehdyttyä Onlive-pilvipelipalveluun. Alkuperäinen aiheeni koski vain pilvipalveluita yleisesti, mutta asiaan tarkemmin perehdyttyäni huomasin aiheen niin laajaksi, että päädyin rajaamaan aiheen pilvipalveluiden tietoturvaan. Tietoturva oli helppo valinta, huomattuani kuinka tärkeänä ja suurena huolena sitä yritysten kannalta pidettiin. Pilvipalveluiden tietoturvasta ei myöskään ole tietääkseni aikaisemmin tehty opinnäytetyötä.

Pilvipalveluista löytyy jo muutama kirja ja runsaasti muuta materiaalia suomenkielellä. Pilvipalveluiden tietoturvaan liittyvä materiaali on kuitenkin suurimmaksi osaksi vain englanninkielellä. Pyrin käyttämään suomenkielisiä lähteitä aina kun mahdollista välttääkseni käännösvirheiden syntymistä. Kaikille englanninkielisille termeille ei löytynyt suoraa vastinetta suomenkielestä. Ongelmaksi muodostui myös aiheen nopea kehitys ja täten löytyneen materiaalin vanheneminen, kun jo pari vuotta vanhat tiedot osoittautuivat vanhentuneiksi.

Monissa pilvipalveluita käsittelevissä teoksissa esitellään ja vertaillaan pilvipalveluntarjoajia. Päätin kuitenkin omasta työstä jättää kyseisen kappaleen tietoisesti pois, koska tieto tarjolla olevista palveluista vanhenee hyvin nopeasti, esimerkiksi Immo Salon vuonna 2010 julkaistussa kirjassa löytyvän palveluntarjoajavertailun hinnoittelut ja tarjolla olevat palvelut ovat suuresti muuttuneet tähän päivään mennessä. Myöskään kaikkia vertailussa mukana olevia yrityksiä ei enää ole olemassa. Kova kilpailu karsii kannattamattomat yritykset pois usein suurempien palveluntarjoajien alaisuuteen sekä pitää hinnoittelun vaihtelevana.

Kaiken kaikkiaan olen tyytyväinen valitsemaani opinnäytetyöaiheeseen ja itse työhön. Vaikka opinnäytetyön tekoon jäänyt aika jäi niukaksi, auttoi tiukka päivittäinen keskittyminen aiheeseen työn parempaan lopputulokseen. Pilvipalveluista on tehtynä jo lukuisia opinnäytetöitä, mutta pidän aihetta niin laajana ja nopeasti kehittyvänä, että siitä irtoaa vielä pitkään hyviä opinnäytetyöaiheita. Pelkästään pilvipalveluiden tietoturvaa käsitteleviä yli 300-sivuisia englanninkielisiä teoksia löytyi useampiakin. Tietoturvaa olisi voinut tutkia esimerkiksi teknisemmin protokolla- ja ohjelmistotasolla tai ottaa kantaa tietoturvaan palveluntarjoajan kannalta.

LÄHTEET

Amazon Web Services. 2013. Amazon Machine Images (AMIs). Luettu 24.4.2013. https://aws.amazon.com/amis/

Arif, M. 2009. A history of cloud computing. Tech Target. Luettu 8.5.2013. http://www.computerweekly.com/feature/A-history-of-cloud-computing

Brodkin, J. 2008. Gartner: Seven cloud-computing security risks. Infoworld. Luettu 18.4.2013. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1

Burns, C. 2012. 10 most powerful IaaS companies. Network World inc. Luettu 20.4.2013. http://www.networkworld.com/supp/2012/enterprise2/040912-ecs-iaas-companies-257611.html

Clabby, J. 2012. Move Over VMware: KVM Has Arrived. Enterprise Systems Media Inc. Luettu 25.4.2013. http://enterprisesystemsmedia.com/article/move-over-vmware-kvm-has-arrived

Cloud Computing – Relevance to Enterprise. 2011. Robiul's Blog. Nähty 4.5.2013. http://robiulislam.wordpress.com/2011/12/28/cloud-computing-for-enterprise/

Cloud Computing Top Threats in 2013. 2013. Cloud Security Alliance. Luettu 5.5.2013. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Five Ways to Protect Against DDoS Attacks. 2013. IT Business Edge. Luettu 4.5.2013. http://www.itbusinessedge.com/slideshows/show.aspx?c=96534

Goodin, D. 2010. Amazon purges account hijacking threat from site, XSS no more. The Register. Luettu 2.5.2013. http://www.theregister.co.uk/2010/04/20/amazon_website_treat/

Henkilötietojen siirto ulkomaille henkilötietolain mukaan. 2010. Tietosuojavaltuutetun toimisto. Luettu 22.4.2013. http://www.tietosuoja.fi/uploads/7nr20lwabx4vu.pdf

Infrastructure as a Service. 2011. pilvilaskenta.wikispace.com. Luettu 20.4.2013. http://pilvilaskenta.wikispaces.com/IaaS+Infrastructure+as+a+Service

Kerner, S. 2013. VMware CEO Aims for 90 Percent Server Virtualization. QuinStreet Inc. Luettu 25.4.2013. http://www.serverwatch.com/server-news/vmware-ceo-aims-for-90-percent-server-virtualization.html

Krebs, B. 2008. Amazon: Hey Spammer, Get Off My Cloud. The Washington Post. luettu 2.5.2013. http://voices.washingtonpost.com/securityfix/2008/07/amazon_hey_spammers_get_off_my.html

Languages. 2013. Heroku dev center. Luettu 26.4.2013. https://devcenter.heroku.com/categories/language-support

Musil, J. 2012. Amazon apologizes for Netflix's Christmas Eve streaming outage. CNET. Luettu 3.5.2013. http://news.cnet.com/8301-1023_3-57561454-93/amazon-apologizes-for-netflixs-christmas-eve-streaming-outage/

Mustonen, J. 2011. Muuttaako pilveen. Tietojenkäsittelyn koulutusohjelma. Oulun seudun ammattikorkeakoulu. Opinnäytetyö.

Mäkelä, V. 2011. Palvelinvirtualisointi Seinäjoen koulutuskuntayhtymässä VMware vSphere -ratkaisulla. Tietojärjestelmäosaamisen koulutusohjelma. Seinäjoen ammattikorkeakoulu. Opinnäytetyö.

Mäntysaari, L. 2012. Pilvet liikkuvat nyt PaaS:n ja IaaS:n tahtiin. Market-Visio Oy. Luettu 27.4.2013. http://www.marketvisio.fi/fi/ajankohtaista/uutiset-marketvisio/1416-pilvet-liikkuvat-nyt-paas-n-ja-iaas-n-tahtiin

PaaS, IaaS ja SaaS: riskit ja suosio. 2012. Nordcloud. Luettu 19.4.2013. http://www.nordcloud.fi/blogi/paas-iaas-ja-saas-riskit-ja-suosio/

Perfecting the Unknown: Cloud Computing. 2012. San Antonio Express-News. Luettu 3.5.2013. http://www.mysanantonio.com/business/article/Perfecting-the-Unknown-Cloud-Computing-4157844.php

Perkiö, A. 2009. Hyvä ennakkosuunnittelu on parasta tietoturvaa. Viestintäharju Oy. Luettu 22.4.2013. http://www.y-leh-ti.fi/arkisto/artikkeli/2641/+Hyv%C3%A4+ennakkosuunnittelu+on+parasta+tietoturvaa

Peter, M. & Timothy, G. 2011. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST. Luettu 30.4.2013. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Platform as a Service. 2011. pilvilaskenta.wikispace.com. Luettu 20.4.2013. http://pilvilaskenta.wikispaces.com/PaaS+Platform+as+a+Service

Rae, I. 2011. Cloud Connect live: Migrating your existing applications to the AWS Cloud. Bit Current. Luettu 2.5.2013. http://www.bitcurrent.com/cloud-connect-live-migrating-your-existing-applications-to-the-aws-cloud/

Rinne, N. 2012. ERP pilvipalveluna. Tietojenkäsittelyn koulutusohjelma. Turun ammattikorkeakoulu. Opinnäytetyö.

Rittinghouse, J. & Ransome, J. 2010. Cloud Computing: Implementation, Management, and Security. USA: Taylor & Francis Group.

Rong, C., Nguyen, S. & Jaatun, M. 2012. Beyond lightning: A survey on security challenges in cloud computing. Elsevier Ltd. Luettu 28.4.2013. http://www.server6.maghalam.com/Be2012121132531.pdf

Salmio, P. 2012. Pilvipalvelut. Tietojenkäsittelyn koulutusohjelma. Turun ammattikorkeakoulu. Opinnäytetyö.

Salo, I. 2010. Cloud computing. Palvelut verkossa. Jyväskylä: WSOYpro Oy.

Schwartz, M. 2012. New Virtualization Vulnerability Allows Escape To Hypervisor Attacks. Information Week Security. Luettu 4.5.2013. http://www.informationweek.com/security/application-security/new-virtualization-vulnerability-allows/240001996

Sippola, J. 2012. Olisiko jo yrityksen aika siirtyä pilveen. Herlevi Capital. Luettu 14.5.2013. http://www.kill4it.fi/blogi/olisiko-jo-yrityksesi-aika-siirtya-pilveen/

The Billion Dollar Lost Laptop Problem. 2010. Ponemon Institute. Luettu 14.5.2013. http://newsroom.intel.com/servlet/JiveServlet/download/1544-16-3132/The_Billion_Dollar_Lost_Laptop_Study.pdf

Top Threats to Cloud Computing V1.0. 2010. Cloud Security Alliance. Luettu 4.5.2013. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Walker-Morgan, D. 2011. Many Amazon cloud users reveal confidential data. Heise Media UK Ltd. Luettu 3.5.2013. http://www.h-online.com/security/news/item/Many-Amazon-cloud-users-reveal-confidential-data-1263704.html

What languages are supported by Google App Engine. 2013. Google Developers. Luettu 22.4.2013. https://developers.google.com/appengine/kb/general#language

Vikasietoiset palvelut. 2013. Planeetta Internet Oy. Luettu 23.4.2013. http://www.planeetta.net/palvelin/vikasietoiset-palvelut.html