VAASAN YLIOPISTO

TEKNIIKAN JA INNOVAATIOJOHTAMISEN

YKSIKKÖ

TIETOJÄRJESTELMÄTIEDE

Arto Saranpää

Pilvipalveluilla ketteryyttä, kustannustehokkuutta ja tietoturvaa
CASE: KEHA-Keskus tietojärjestelmät

Tietojärjestelmätieteen
Pro Gradu- tutkielma

VAASA 2019

SISÄLLYSLUETTELO sivu

KUVA- JA TAULUKKOLUETTELO sivu

LYHENTEET

ACL	Pääsynvalvontaluettelo
ARP	Loogisen verkko-osoitteen selvitysprotokolla
AWS	Amazon pilvipalveluympäristö
BOT	Botti-verkko, jota voidaan käyttää palvelunestohyökkäyksissä
DDoS	Hajautettu palvelunestohyökkäys
DMZ	Organisaation edustaverkko internet-rajapinnassa
DoS	Palvelunestohyökkäys
GDPR	Yleinen tietosuoja-asetus
IaaS	Infrastruktuuri palveluna
IDS	Tunkeutumisen havaitsemisjärjestelmä
IP	Internet-kerroksen protokolla
IPS	Tunkeutumisen suojausjärjestelmä
IPsec	Internetprotokollan salaus
On-Premise	Paikallinen konesali vrt. pilvipalvelu
PaaS	Sovellusalusta palveluna
RRAS	Reititys- ja etäkäyttöpalvelu
SaaS	Sovellus palveluna
SHA	Salausalgoritmi
SLA	Palvelutasosopimus
UDR	Spesifinen tietoliikennereititys
VPN	Virtuaalinen erillisverkko, joka on erotettu muusta julkisesta liikenteestä

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen yksikkö
Tekijä: Arto Saranpää
Tutkielman nimi: Pilvipalvelulla ketteryyttä, kustannustehokkuutta ja tietoturvaa tietojärjestelmiin CASE: KEHA-keskus tietojärjestelmät
Ohjaajan nimi: Teemu Mäenpää
Tutkinto Kauppatieteiden maisteri
Oppiaine: Tietojärjestelmätiede
Opintojen aloitusvuosi: 2015
Tutkielman valmistusvuosi: 2019 **Sivumäärä:** 60

TIIVISTELMÄ:

Tämä tutkielma käsittelee pilvipalveluita ja niiden käyttöä KEHA-keskuksessa. Tutkimuksen tavoitteena on selvittää pilvipalveluiden käytön tuomat edut ja mahdolliset haitat case-yritykselle verrattuna perinteisiin konesaliratkaisuihin verrattuna. Aihe on rajattu pilvipalveluiden käyttöä tietoturvan, ketteryyden ja kustannustehokkuuden näkökulmasta, jotka ovat olleet keskeisenä osana KEHA-keskuksen pilvipalvelustrategiaa. Tutkielman yhtenä tarkoituksena on tunnistaa pilvipalvelun vahvuudet verrattuna perinteisiin konesaleihin verrattuna. Tutkielmassa esitellään tutkimuksen kannalta oleellista teoriaa, sekä selvitetään pilvipalveluiden käyttöä käytännössä.

Työ suoritetaan tapaustutkimuksena, jossa tarkastellaan aiempia tutkimuksia pilvipalveluja hyödyntävistä organisaatioista. Lähdemateriaalina tutkielmassa käytetään aiheesta löytyvää kirjallisuutta, tieteellisiä artikkeleita ja julkaisuja, sekä käytännön kokemusta. Käytännön kokemus tulee tutkielman tekijän omakohtaisen kokemuksen avulla. Myös pilvipalvelujen käytöstä on kertynyt materiaalia KEHA-keskukselle, jota hyödynnetään tässä tutkimuksessa.

Pilvipalveluiden hyödyntäminen on yrityksille tai organisaatioille erittäin hyvä vaihtoehto entisiin teknologioihin verrattuna. KEHA-keskuksen tapauksessa pilvipalvelun käyttö on ollut helppoa, tehokasta, joustavaa sekä luotettavaa. Pilvipalveluita on kyetty hyödyntämään KEHA-keskuksen tietojärjestelmissä erittäin hyvin ja palveluun ollaan tyytyväisiä niin työntekijöiden kuin johtoryhmän suunnalta.

AVAINSANAT: Pilvipalvelut, Azure, IaaS, PaaS, SaaS, Tietoturva

UNIVERSITY OF VAASA
Technology and innovations
Author: Arto Saranpää
Topic of the Thesis: Cloud Services produce flexibility, cost efficiency and security for IT-systems CASE: KEHA-center information systems
Name of the Supervisor: Teemu Mäenpää
Degree: Master of Science in Economics and Business Administration
Major Subject: Computer Science
Year of Entering the University: 2015
Year of Completing the Thesis: 2019 **Pages**: 60

ABSTRACT:

This thesis deals with cloud services and their use at the KEHA Center. The aim of the study is to find out the benefits of the use of cloud services and the potential disadvantages to the case company compared to conventional data solutions. The subject is limited to the use of cloud services from the point of view of security, agility and cost-effectiveness, which have been an integral part of the KEHA Center's cloud hosting strategy. The purpose of the thesis is to identify the strengths of the cloud service compared to the traditional datacenters. The thesis presents a theory relevant to research and explores the use of cloud services in practice.

The work is carried out as a case study examining previous surveys of cloud computing organizations. The source material used in the thesis is literature, scientific articles and publications, as well as practical experience. Practical experience comes with the author's personal experience. Also, the use of cloud services has accumulated material for the KEHA Center, which is used in this study.

Utilizing cloud services for companies or organizations is a very good alternative to existing technologies. In the case of the KEHA Center, the use of the cloud service has been easy, efficient, flexible and reliable. The cloud services have been utilized very well in the information systems of the KEHA Center, and the service has been satisfied with both employees and the management team.

KEYWORDS: Cloud service, Azure, IaaS, PaaS, SaaS, Cloud security

1 JOHDANTO

Yritysten ja organisaatioiden palvelut, ja niiden käyttö ovat viime aikoina siirtyneet yhä vahvemmin käyttämään pilvipalveluita. Suomen yrityksistä yli 50% ovat siirtyneet käyttämään pilvipalveluita (Tilastokeskus 2014). Tieto siitä, että organisaation tietoja tallennetaan pilveen ja jonka todellista sijaintia ei välttämättä tiedetä, saattaa aiheuttaa organisaatiossa epävarmuutta pilvipalvelujen käyttöön.

Todellisuudessa pilvipalveluita tuottavat yritykset ovat panostaneet merkittävästi tietoturvaan. Mikään yksittäinen valtiohallinnon organisaatio tai pieni palveluntuottaja ei pysty samanlaiseen tiedon ja infrastruktuurin suojaamiseen, koska siihen tarvitaan merkittäviä taloudellisia panostuksia sekä erityislaatuista osaamista.

Pilvipalveluiden käyttöä ja käytön esteitä on tutkittu aiemminkin. Tulokset osoittavat, että tietoturva, tiedon eheys ovat huolen aiheista merkityksellisimpiä, kun organisaatiot miettivät pilvipalveluiden käyttöönottoa (Tilastokeskus 2014).

Tarkentavaa ja tuoreempaa tietoa pilvipalvelun käytöstä toimialoittain antaa Radarin, Tiedon, VMwaren Cloud maturity Index -tutkimus (2017), joka toteutettiin verkkokyselyinä ja haastatteluina. Kysely tehtiin pohjoismaisena tutkimuksena ja siihen osallistui 268 yksityisen ja julkisen sektorin päättäjää kattavasti Suomesta, Ruotsista ja Norjasta.

Tutkimuksessa todetaan, että Suomalaisyrityksistä ja julkisyhteisöistä 85% käyttää pilvipalveluita, ja kasvua on tapahtunut yli 30% edelliseen tutkimukseen verrattuna, joka suoritettiin vuonna 2015 (Radar ym. 2017: 11). Kun verrataan kasvua tilastokeskuksen antamiin vuoden 2014 lukuihin, niin voidaan todeta näiden kahden tutkimuksen täydentävän ja tukevan toisiaan käytön kasvua tarkastellessa. Vuosien 2014 ja 2017 välisenä aikana pilvipalvelujen käyttö on lisääntynyt n. 10-15% vuosittain yrityksissä ja julkisella sektorilla.

Yrityksistä ja julkisen sektorin toimijoista suurin osa on pilvipalvelujen käytössä perustasolla (Basic 46%). Tarkoittaa sitä, että organisaatio käyttää pilvipalvelua yhden palvelun osalta ja jota ei ole integroitu organisaatio toisiin järjestelmiin. Yleisenä ajurina on ollut kustannusten alentaminen yksittäisen palvelun osalta, eikä välttämättä mikään IT-strategian toimeenpaneminen.

Osaavalla (Proficient 29%) tasolla olevalla organisaatiolla on jo jonkin-näköinen pilvipalvelustrategia ja organisaation tuottamat pilvipalvelut ovat linjassa asetetun strategian kanssa. Osaavalla organisaatiolla on useampia palveluita ympäristössä ja käytössä erilaisia palvelumalleja (IaaS, PaaS ja SaaS).

Kypsällä (Mature 14%) organisaatiolla pilvipalvelut on selkeästi määritelty ja IT-toiminnot on viritetty tehokkaiksi. Pilvipalveluihin liittyvät komponenttihankinnat ovat täysin strategian mukaisia. Avainajurit ovat kehitys, muutos ja innovaatiot.

Epäkypsillä (Immature 11%) organisaatioilla ei ole ollenkaan pilvipalvelustrategiaa. Heillä ei ole kompetenssia, osaamista tai kyvykkyyttä ottaa käyttöön pilvipalveluita. Pilvipalvelun käyttö on hyvin vähäistä, jos ollenkaan. Epäkypsissä organisaatioissa suurimmaksi esteeksi palvelun käyttöönotossa koetaan palvelun turvallisuus ja siihen liittyvät säänteleyt tai asenteet (Radar ym. 2017: 14).

Erityisesti julkisella sektorilla on merkittäviä haasteita vastata kasvavaan palvelutarpeeseen. Esimerkkinä väestön ikääntyminen tuo itsestään jo kustannusmenoja julkiselle sektorille, jossa palveluja pitäisi pystyä automatisoimaan tulevaisuutta silmällä pitäen. Digitalisointi nähdään yhtenä tärkeimmistä toimenpiteistä, jotka tulevat mahdollistavat tuottavuuden lisäämisen julkisen sektorin palveluissa. Julkisen sektorin pilvipalvelujen kehittymistä esimerkiksi finanssialan pilvipalvelujen käyttöön verrattuna, on julkinen sektori ottanut harppauksia eteenpäin ja kuronut kiinni umpeen välimatkaa kahden vuoden aikana. Valtiohallinnon yhtenä kärkihankkeena on ollut juurikin digitalisaation kehittäminen ja edistäminen. Tämä alkaa väistämättä näkymään tutkimuksissa ja tosielämässä.

1.1 Tausta

Tämän tutkimuksen aiheena on pilvipalvelun hyödyntäminen tietojärjestelmiä tuottavassa organisaatiossa. Tutkittavana ilmiönä on KEHA-keskus organisaation tietoturvan varmistaminen sen tuottamista pilvipalveluista. Se ajuri miksi palvelut ovat kiinnostavia KEHA-keskuksen näkökulmasta on se, että se tarjoaa ketterämmän ja jossain tapauksissa kustannustehokkaamman vaihtoehdon perinteisiin konesaleihin verrattuna.

KEHA-keskus on organisaatio, joka tuottaa sähköisiä palveluita pääasiassa ELY-keskuksille ja TE-toimistoille eli kansalaisille tunnetumpi TE-palvelut virasto. KEHA-keskus tuottaa myös valtionhallinnon muille organisaatiolle sähköisiä palveluita joissain määrin.

Valtiohallinnon virastot tuottavat toiminnallaan paljon suojattavaa tietoa. Suojattava tietoa organisaatio saa kansalaisilta erilaisten hakemusten ja ilmoitusten myötä, joita organisaatiot saavat sekä sähköisesti ja paperisena. Lopullisesti tiedot tallennetaan organisaatoissa sähköisen asianhallintajärjestelmään. Useinkin organisaation asianhallinta-järjestelmät ovat päivittäisen toiminnan ydin, joihin kohdistuu tietoturvan ja toimintavarmuuden osalta suurimmat vaatimukset.

KEHA-keskuksella on kokemusta perinteisistä konesalipalveluista ja niiden rinnalle on haluttu toimivat pilvipalveluympäristöt.

1.1.1 Perinteiset konesalipalvelut

Perinteisiä konesaleja ajetaan normaalisti toimittajan tiloissa olevista konesaleista tai asiakkaan omissa tiloissa olevasta konesalista. Pilvipalvelujen myötä näitä ratkaisuja on alettu kutsumaan On-Premise tai On-Site ratkaisuiksi.

Pääsääntöisesti nämä konesalit tarjoavat kapasiteettiresursseja virtuaalipalvelimina tai toisena vaihtoehtona tietylle palvelulle tai asiakkaalle dedikoituja palvelimia. Tämän

tyyppinen kapasiteettitarjonta tarvitsee toimiakseen luotettavat ja turvalliset tilat palvelimille, jossa tulee ottaa huomioon jäähdytys, varavoima, sähkönkulutus sekä jatkuvuuteen liittyviä seikkoja.

Nämä tarvitsevat myös aina luotettavat ja vakaat tietoliikenneyhteydet, palomuurit sekä konesalin lähiverkkoinfrastruktuurin. Näistä edellä mainituista komponenteista syntyy jo itsessään iso kustannustekijä ennen ensimmäistä palvelinta ja sen päällä pyörivää sovelluspalvelua.

Toimittajan On-Premise ratkaisuissa palvelinten ja lisäpalveluiden käyttöönotosta sovitaan aina erikseen asiakkaan kanssa, jossa määritellään palvelutasot (Service Level Agreement), hallinta, valvonta sekä vastuut. Tässä mallissa IT-palveluja tuottava organisaatio kärsii tämän mallin kankeudesta.

Tietojärjestelmän kehitysvaiheessa, joista yleensä vastaa organisaation kehitys – ja suunnittelutiimit kärsivät eniten palvelinten hitaasta toimituksesta sekä käyttöönotosta. Näissä tapauksissa se voi tarkoittaa viikkojen jopa kuukausien viitettä tietojärjestelmäprojektin alkuvaiheessa (Prashant 2003: 10).

Käytännön kokemus osoittaa, että palveluntarjoajat tilaavat palvelimia sitä mukaa kun niitä tarvitaan. Tämä on osoittautunut yhdeksi merkittäväksi pullonkaulaksi tietojärjestelmäprojektien alkuvaiheessa (A1 2002: 50).

1.1.2 Pilvipalvelujen historia ja sen yleispiirteet

Digitalisaation alkulähteet sijoittuvat 1950-luvulle, jolloin tietokoneet keksittiin. Jo 1960 luvulla tietokoneiden laskentakapasiteettiä käytettiin pilvipalvelun kaltaisella tavalla, vaikka pilvipalvelu terminä ei ollut vielä siihen aikaan käytössä.

Silloin käytettiin suuria ja kalliita tietokoneita laskentakapasiteettina jaettuna resurssina, joita useammat yritykset pystyivät käyttämään yhtä aikaa. Kuitenkin siihen aikaa tietoliikennenopeudet olivat hitaita ja kapasiteetin käyttö koitui hankalaksi (Heino 2010: 32).

1990-luvulla digitalisaatio otti harppauksen eteenpäin ja erilaisia verkon päälle rakennettuja palveluita alkoi syntyä vauhdilla. 2000-luvulla syntyi pilvipalveluiden todellinen läpimurto ja alalle puski uusia menestyviä yrityksiä sekä palveluita kuten Google, Facebook, Amazon, Salesforce (Heino 2010: 110).

Pilvipalveluiden viimeinen murtovaihe oli 2000-luvun puolivälissä, jolloin suuret palveluntarjoajat alkoivat tarjoamaan laskenta- ja tallennuskapasiteettia internetin välityksellä. Tämä edellytyksenä oli teknologian jalostuminen riittävä korkealle tasolla, jotta sitä voitaisiin käyttää selainrajapinnan avulla. Keskeisenä tekijänä teknologisesta näkökulmasta oli se, että palvelinvirtualisointi, tietoliikenne sekä muut perusinfrastruktuuri olivat riittävällä tasolla, jotta palvelua voidaan käyttää luotettavasti.

Yllä mainitut yritykset ajoivat jo tuohon aikaan ympäristöjään virtualisoinnin avulla ”always on” periaatteella. Näin ympäristöä voidaan päivittää sekä vaihtaa komponentteja ilman käyttökatkoja. Yhtenä tärkeänä tekijänä myös skaalautuvuus palvelun kuormituksen mukaan. Nämä yllä mainitut ominaisuudet ovat keskeinen fundamentaalinen perusta pilvipalvelujen tuottamisesta asiakkaille luotettavasti (Brian ym. 2012: 4).

1.2 Tutkimusongelma ja työn viitekehys

Aikaisemmin KEHA-keskuksen järjestelmiä on tuotettu perinteisin konesalimenetelmin, jossa palveluita on sijoitettu valtion omistamiin konesaleihin tai palvelutarjoajien konesaleihin. Käytäntö on osoittanut sen, että perinteiset konesalipalvelut eivät vastaa nykypäivän ketterän kehityksen maailmaan, jossa tietojärjestelmäprojektien syklit ovat tiheät. Virtuaalipalvelimen ja sovellusalustojen tilaaminen, sekä käyttöönotto on hidasta perinteisessä konesalimenetelmässä.

Perinteisessä mallissa organisaation konesalitiimille tai palveluntarjoajalle selvitetään tarvittava laitekokoonpano, muistin määrä, prosessorien teho, levykoko yms. tulee ottaa huomioon jo tässä vaiheessa. Tutkimuksissa voidaan osoittaa, että pilvipalvelut ovat ketterämpiä ja nopeampia ottaa käyttöön vrt. perinteiset konesalipalvelut (Mccrea 2013: 42; Winkler 2011: 32).

1.3 Tutkielman tavoitteet ja rajaukset

Tämän työn tavoitteena on todentaa hypoteesi siitä, että pilvipalveluista saatava hyöty KEHA-keskukselle on ollut ja on tulevaisuudessa järkevä vaihtoehto tuottaa tietojärjestelmäpalveluja nyt ja tulevaisuudessa. Vuonna 2014 KEHA-keskuksen tekninen tiimi arvioi, että pilvipalvelujen käyttöönotto toisi etua perinteisiin konesaliratkaisuihin verrattuna. Tästä voidaan johtaa tutkimuskysymys:

Millä teknisillä ratkaisuilla KEHA-keskus saavuttaa pilvipalvelun tarjoamat hyödyt?

Tutkimuskysymyksellä yritetään saada vastaus siihen, onko aiemmat olettamukset pilvipalvelujen eduista relevantteja verrattuna perinteisiin konesaliratkaisuihin. Potentiaalista hyötyarvoa voi olla monenlaista. Esimerkiksi Infrastructure as a Service (IaaS)- palvelumallissa palvelinten asentaminen ja hallinta, kustannusrakenne-erot perinteisen ja pilvikonesalin välillä, jossa maksetaan palvelimen käytöstä käyttöajan mukaan sekä palvelinten lisenssikulut yksinkertaistuvat, koska ne ovat sisäänrakennettuna kk-hinnassa.

Toisena esimerkkinä Platform as a Service (PaaS)- palvelumallissa, jossa palvelin- ja käyttöjärjestelmäkerros (IaaS) jää palveluntarjoajan vastuulle. Tässä palvelumallissa kustannus- ja ketteryyspotentiaali on vieläkin isompi verrattuna IaaS- palvelumalliin. PaaS eli sovellusalusta palveluna tarjoaa valmiin sovellusalustan, jonka päälle voidaan lähteä ketterästi ja kustannustehokkaasti lähteä rakentamaan palveluita pienellä alkuvalmisteluun liittyvällä työpanoksella. IaaS- ja PaaS- palvelumallin skaalautuvuus on myös huomattavasti yksinkertaisempaa, kustannustehokkaampaa ja ketterämpää perinteiseen konesaliin verrattuna.

Nämä yllä mainitut edut tuovat tietojärjestelmäkehitykseen etuja, koska projektin vaatimat resurssit ovat nopeammin käyttöönotettavissa. Projektien aikana tuleviin muutostarpeisiin voidaan vastata ketterämmin ja näin ollen tällä on positiivisia vaikutuksia projektien aikatauluihin.

Tutkielma on rajattu KEHA-keskuksen tieto- ja viestintäyksikön tuottamiin tietojärjestelmiin. Pilvipalvelussa tuotettavat tietojärjestelmät on sijoitettu Microsoft Azure- palveluun, näin työssä tarkastellaan pilvipalveluita MS Azuren näkökulmasta.

Tietoturvan osalta tutkimuksessa tarkastellaan Azuren omilla komponenteilla rakennettuja tietoturvaratkaisuja KEHA-keskuksen pilvipalveluympäristössä. Azuren kolmannen osapuolen tarjoamat lisämaksulliset komponentit eivät ole tässä tutkimuksessa tarkastelun piirissä.

1.4 Työn rakenne

Tutkielman ensimmäisessä kappaleessa käydään läpi johdantoa, jossa käsitellään pilvipalvelujen taustaa. Ensimmäisen kappaleen alaluvuissa käsitellään tutkielman taustaa ja sen viitekehystä. Tutkimusmenetelmät, tutkimusongelma ja sen rajaus. Ensimmäisessä kappaleessa kuvataan myös keskeiset käsitteet, tavoitteet ja työn rakenne.

Toisessa luvussa käydään läpi kirjallisuuskatsausta pilvipalveluista. Pilvipalvelun keskeiset käyttöönottomallit sekä pilvipalvelujen käyttöönottomalleja tarkastellaan tässä luvussa. Nämä ovat tutkielman viitekehyksen keskiössä ja ne kuvataankin tarkalla tasolla.

Tutkielman kolmannessa luvussa käydään läpi tutkimuksen kohteena olevan KEHA-keskuksen tietojärjestelmiä. Tässä käydään läpi koko hybridi-infrastruktuurin hallintamalli, joka sisältää niin perinteisen, kuin pilvipalvelu infrastruktuurin.

Neljännessä luvussa esitetään työn tulokset ja vastataan asetettuun tutkimusongelmaan. Viidennessä ja kuudennessa luvussa pohdinta, johtopäätökset sekä yhteenveto.

2 PILVIPALVELUIDEN KÄYTTÖ ORGANISAATIOISSA

Seuraavissa kappaleissa käsitellään aiempia tutkimuksia aiheesta. Tässä kappaleessa käydään läpi kirjallisuudesta sekä artikkeleista löytynyttä tietoa pilvipalveluista, niiden riskeistä, hyödyistä.

Kuten johdannossa mainittiin, pilvipalvelujen käyttö on lisääntynyt räjähdysmäisesti, niin yksityisellä kuin julkisella sektorilla. Pilvipalvelujen tarjoaa modernin tuotantomallin IT-palvelulle ja se sisältää tyypillisesti internetin yli tarjottavia on-demand palvelua, ja joka on dynaamisesti skaalautuva ja joustava käyttämällä virtuaalisia resursseja.

Näiden ominaisuuksien avulla pilvipalvelut antavat yrityksille ja tietotekniikkateollisuudelle mahdollisuuden tarjoamalla resurssien nopean käyttöönoton, joustavasti, skaalautuvasti ja kustannustehokkaasti.

Vaikka pilvipalvelut tarjoavat etuja ja kustannustehokkaita vaihtoehtoja IT-palvelulle sekä antavat laajennusmahdollisuuden. Siltikin uudet riskit on tiedostettava ja mahdollisuudet tietoturvan parantamiseen kannattaa ottaa käyttöön pilvipalvelussa (Carroll, M. ym. 2011: 1).

Vaikka nämä pilvipalvelujen komponentit ja ominaisuudet tarjoavat ratkaisuja IT - ongelmiin sekä tarjoavat monia etuja, niin pilvipalvelun käyttö ei ole riskitöntä ja täysin turvallista sellaisenaan.

Tavallisesti yrityksen tietohallintojohto tietoturvapäällikkö johdolla vastaavat tietoturvariskeistä suojellakseen palveluita ja siellä olevaa dataa. IT-palvelun hallintatapa ja riskienhallinta nousevat tärkeään rooliin pilvipalvelun hallintaprosessissa.

Hallintatapa pannaan täytäntöön tietoturvapolitiikan ja prosessien kautta. Näiden käytäntöjen ja menettelyjen tulisi noudattaa parhaita käytäntöjä ja niiden olisi oltava yhdenmu-

kaisia yrityksen IT-strategian kanssa. Myös riskien tunnistaminen ja analysointi on tärkeää asettaa etusijalle pilvipalvelun toteutuksessa. Toteutetun pilvipalvelun tarkasteleminen ja auditointi ovat tärkeä osa yrityksen IT-strategiaa ja noudattavat näin parhaita käytäntöjä.

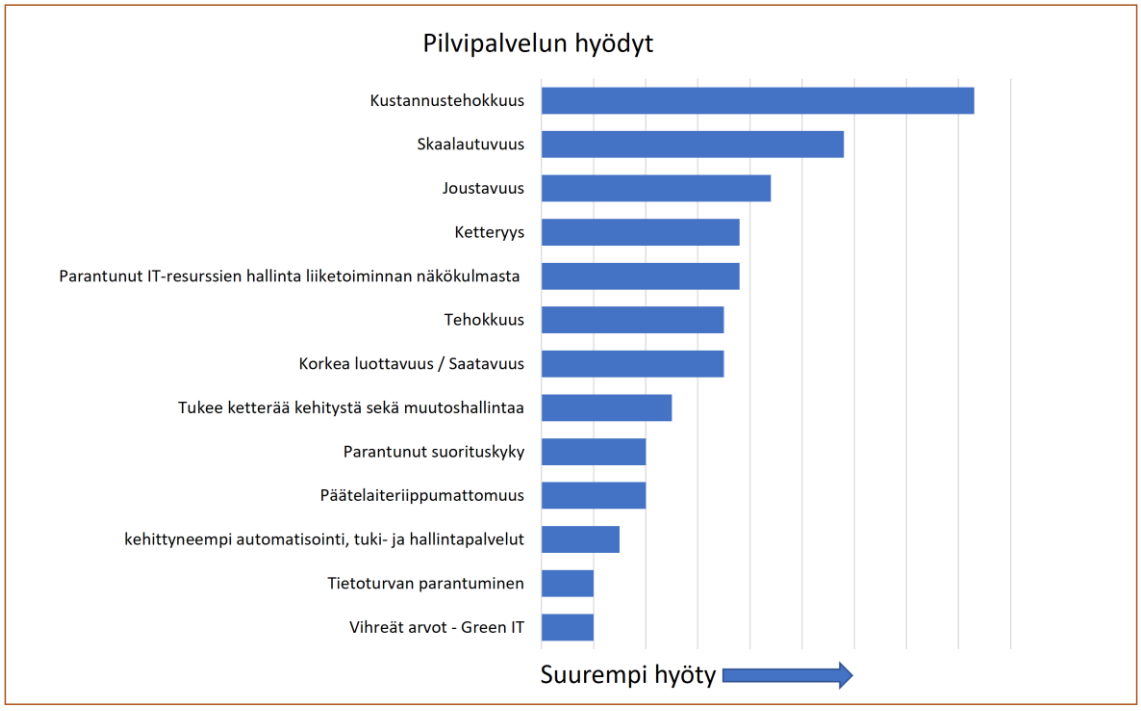
Riskien tunnistaminen ja riskianalysoinnin tulisi olla suunniteltu ja toteutettu sen varmistamiseksi, että tarvittavat toimet tukevat riskienhallinnan, yritystoimintaan ja IT-strategian tavoitteita (Carroll, M. ym. 2011: 2).

Pilvipalvelut tarjoavat säästöjä tietotekniikan kustannuksiin, mukaan lukien pienemmät suunnittelu-, toteutus-, ja ylläpitokustannukset. Vähemmän ostettavaa laitteistoa sekä siihen liittyviä tuki-, ja varaosapalveluita.

Lisäksi merkittäviin resurssikustannuksiin voidaan laskea sähkö, jäähdytys ja konesalitila. Kun nämä edellä mainitut kustannustekijät on ”siirretty” pilvipalveluntarjoajalle se vähentää organisaation toimintakustannuksia ja resurssista maksetaan vain todellisen käyttöasteen mukaan.

Yllämainitun laitteistoista aiheutuvien kulujen lisäksi pilvipalveluiden avulla säästöjä syntyy sovelluskehitysprojekteissa, missä saadaan ketterästi käyttöön tarvittavat resurssit ja komponentit. Näin projekti ei pysähdy alkuvaiheessa laitehankintoihin liittyviin viiveisiin (Carroll ym. 2011: 2).

Etelä-Afrikan Pretorian yliopiston tekemä kirjallisuus- ja haastattelututkimus (Carroll ym. 2011) pilvipalvelujen hyödyistä ja riskeistä osoittaa sen, että suurimmat vaikutukset ja hyödyt ovat kustannustehokkuus, skaalautuvuus, joustavuus ja ketteryys, joita tässä tutkielmassa erityisesti tarkastellaan.



Kuva 1. Pilvipalvelujen hyödyt (Carroll ym., 2011).

Tutkimuksen kirjallisuuskatsauksen osuudessa suurimman painoarvon hyötynäkökulmasta katsottuna sai kustannustehokkuus, jonka katsottiin tutkimuksen perusteella olevan suurin saavutettava hyöty. Tutkimuksessa hieman yllättäen kehittyneempi automatisointi ei saanut niin suurta painoarvoa, vaikka juuri sen avulla saadaan parannettua kustannustehokkuutta mm. palvelinten käyntiaikojen automatisoinnilla (Start/Stop VMs during off-hours solution in azure automation, 2017).

Tutkimuksen ajankohdan aikaan, vuonna 2011 teknologia ei välttämättä ollut vielä niin kypsää, että automatisoinnille oltaisiin voitu antaa isoa edes suurta painoarvoa.

Toisessa Aleem & Sprottin (2013: 9) tutkimusanalyysissä keskeiseksi hyödyksi nousi resurssien tehokkaan käytön. Palvelun skaalautuvuus ilman merkittäviä taloudellisia panostuksia on mahdollinen pilvipalveluskenaariossa ja palvelujen virtualisointi redundanssin vähentämiseksi on kannustin monille yrityksille toteuttaa pilvialustoja.

Kyky nopeuttaa datan haku- ja suoritusaikaa on myös tärkeä merkitys pilvialustoihin siirtyneillä organisaatioilla. Washington Post on mm. saanut etua pilviteknologiasta, jonka internetsivujen hakuajat ovat pienentyneet merkittävästi.

Toisessa esimerkissä "Internet Movie Database" (IMDB) käyttää Amazonin (AWS) ja Googlen (Google Cloud Platform) pilvialustoja. Esimerkkinä käyttämällä Amazonin CloudFrontia, he ovat onnistuneet vähentämään laitteistokustannuksia ja haut/pääsyt verkkosivustoin ovat nopeutuneet. Liikenteen ollessa jopa 2.3 miljoonaa pyyntöä päivässä. Ja tämä liikennemäärä syntyy pelkästään älypuhelimista, jotka voivat helposti lisätä kuormitusta IMDB-palvelimiin. Siirtämällä haku- ja videotiedostot CloudFront palveluun, on käytännössä vähentänyt palvelinten ylläpidon minimiin ja taas luotettavuus on noussut merkittävästi palvelussa.

Aleem & Sprott nostivat esiin myös laitteiston korjauspäivittämisen ”Patch Management”. Se on organisaation IT-osaston ydintoimintoja ja haavoittuvuuksia on välttämätöntä korjata ennen niiden hyödyntämistä. Tämä voi olla erittäin kallista toimintaa silloin kun organisaatiossa on käynnissä useita keskeisiä yrityssovelluksia useissa eri versioissa ja niissä on erilaiset käyttöjärjestelmäversiot.

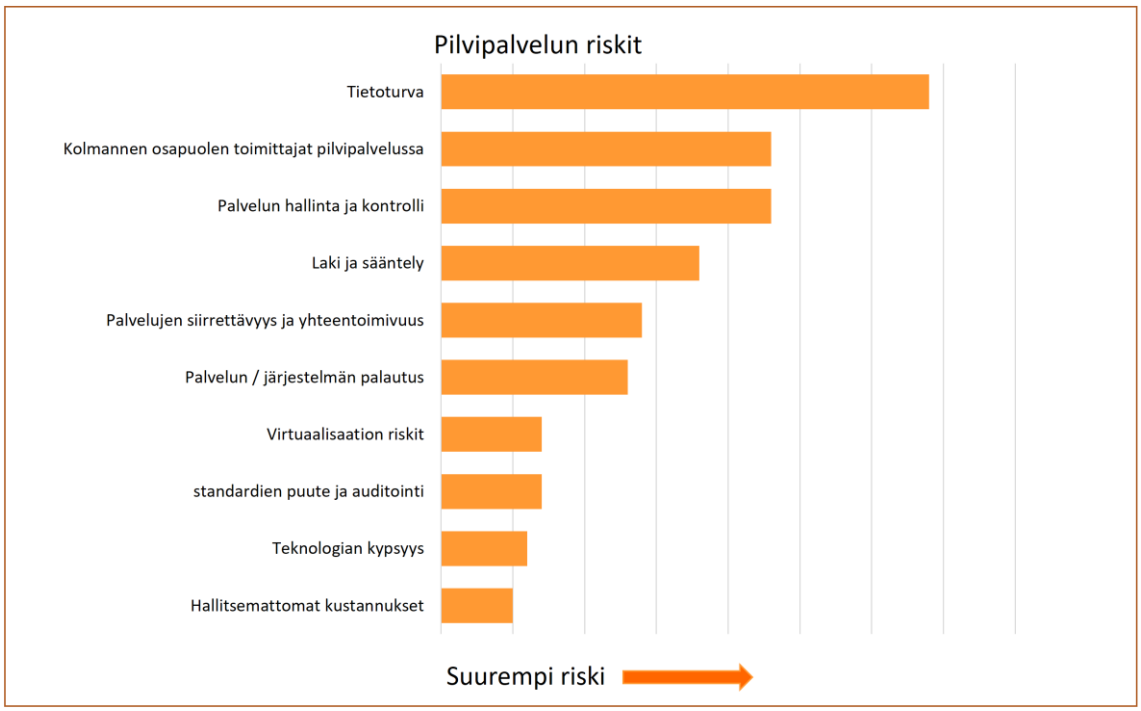
Myös yksi pilvialustan eduista on tietojen varastointi (varmuuskopiointi) ja toipumissuunnitelman implementoiminen pilvipalveluun (Disaster Recovery). Monet pilvipalvelutarjoajat tarjoavat nykyään edullista datan tallennustilaa (Cloud Storage) pilvestä, joten nämä edellä mainitut toimenpiteet ovat järkevä toteuttaa pilvialustalla.

Vaikka pilvistrategiaa puoltavia ajureita syntyy organisaatioissa, niin pilvipalvelu ei ole täysin riskitön tai turvallinen. Pilvipalvelujen perusteellinen ymmärrys ja tietoturvariskien lieventäminen on tärkeä askel, kun organisaatio harkitsee tai on ottamassa käyttöön pilvipalveluita. Kuva 2. esittää kirjallisuuskatsauksessa esille nousseet riskit.

Suurimpana huolena nähtiin turvallisuus tai tietoturvallisuus, miten se halutaan esittää. Kun sovellukset ja data on ylläpidossa palveluntarjoajalla, niin data ei ole enää omassa

hallinnassa ja on näin alttiina haavoittuvuuksille. Hosting sovellukset (PaaS) ja data jaetussa infrastruktuurialustassa kasvattavat mahdollisuutta luvattoman pääsyn dataan. Nämä nostavat huolenaihetta esimerkiksi, yksityisyydestä, identiteetin hallinnasta, pääsyn todentamisesta, luottamuksellisuudesta, tiedon eheydestä, tietojen saatavuudesta, tiedon salauksesta, verkon turvallisuudesta ja fyysisestä turvallisuudesta.

Turvallisuuden lisäksi riskejä ja muita huolenaiheita ovat SLA (palvelutaso), kolmannen osapuolen palveluntarjoaja, hallinta, lukittautuminen yhteen toimittajaan (Vendor lock-in), palvelun laatu, toimittajan elinkaari/elinkelpoisuus, tietojen ja sovellusten hallinta ja valvonta, työkuorman hallinta, suorituskyky, muutoksen hallinta, palvelun saatavuus, puuttuvat työkalut hallintaan ja seurantaan, palvelun avoimuus, lakien ja sääntelyn noudattaminen, palvelujen siirrettävyys ja yhteen toimivuus, palvelun tai järjestelmän palautus, virtualisoinnin riskit, standardien ja auditoinnin puute, teknologian kypsyys ja hallitsemattomat kustannukset (Carroll ym. 2011: 4).



Kuva 2. Pilvipalvelujen riskit (Carroll ym., 2011).

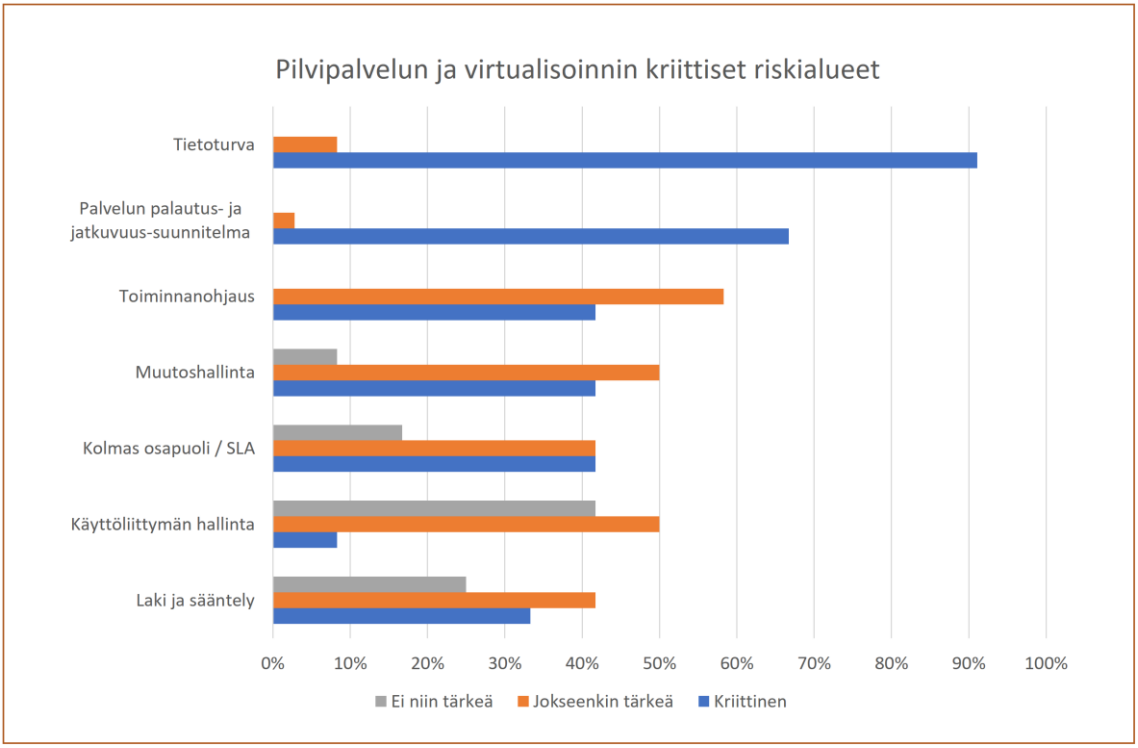
Samankaltaisia tuloksia saatiin haastattelu tutkimuksessa, johon osallistui 15 eri organisaatiota, niin julkishallinnosta kuin yksityiseltä sektorilta. Vastaajista liki 92% piti suurimpana riskinä tietoturvaa.

Pilvipalvelun palautus- ja jatkuvuussuunnitelman puuttumista toiseksi merkittävimpänä riskinä, jossa jokainen vastaus oli jokseenkin tärkeä tai kriittinen. Vastaajista liki 67% pitivät tätä kriittisenä riskitekijänä. Yli 80% vastaajista olivat sitä mieltä, että kolmannen osapuolen palvelut ja niihin liittyvät riski olivat jokseenkin tärkeitä tai kriittisiä. Käyttöliittymän hallintaa pidetiin vähiten merkitsevänä riskitekijänä, sekä lakia tai sääntelyä ei pidetty voimakkaan kriittisenä riskialueena.

Myös Aleem & Sprottin (2013) tutkimusanalyysissä todettiin saman suuntaista. Tutkimusanalyysissa korostettiin, että suurimpiä huolenaiheita oli turvallisuus (93,8 prosenttia), palvelun hallinta (61,1 prosenttia) ja palvelun valvonnan puute (56,6 prosenttia).

Tutkimuksessa korostettiin, että suurin osa pilvipalvelun ylläpitäjistä eivät olleet tietoisia siitä, että jotkut pilvipalvelun tarjoajat hallitsevat tällä hetkellä salauksen purkuavaimia, joiden avulla ne voivat purkaa asiakkaansa tiedot.

Tätä voidaan lähtökohtaisesti pitää tärkeänä turvallisuusongelmana, ja se on yksi niistä tekijöistä, joita on tarkasteltava palvelusopimuksen määrittämisvaiheessa (SLA). Tietojen menetystä ja tietovuotoja (73,5 prosenttia) pidettiin myös selkeänä uhkana pilvipalveluissa. Myös palvelun ja liikenteen kaappausta (60,8 prosenttia) pidettiin selkeänä uhkana organisaation pilvikäytössä.



Kuva 3. Pilvipalvelun kriittiset riskialueet (Carroll ym. 2011).

Nämä yllä esitellyt tutkimukset (Kuva 3.) osoittavat, että on tärkeää varmistua siitä, että pilvipalvelunympäristö on suojattu riittävällä tasolla ja sitä on näin ollen mahdollista käyttää turvallisesti. Pilvipalvelun valvonnan luominen tärkeää pilvipalvelun turvaamisen näkökulmasta (Carroll ym. 2011: 4).

Aiempia tutkimuksia ja artikkeleita pilvipalvelujen tietoturvasta, kustannustehokkuudesta ja ketteryydestä löytyy eri tietokannoista. Pilvipalvelut eivät itsessään tuo välttämättä kustannustehokkuutta vaan se, että miten ja millä pilvipalvelusta on saatavilla laskentakapasiteettia. Tämän toteaa myös Gmach, D., Rolia, J., Cherkasova, L (2012) omassa tutkimuksessaan, jossa vertailtiin eri pilvilaskennan tehokkuuden kustannusten malleja. Useimmat palveluntarjoajat tarjoavat staattisesti konfiguroituja virtuaalipalvelimia. He vertailevat tätä T-paidan mitoitukseen, jossa verrataan sitä niin, että mitä suurempi koko, niin sitä enemmän virtuaalipalvelimesta maksetaan.

Jotkut palveluntarjoajat tarjoavat vain staattisen virtuaalipalvelimen mitoituksen, jossa sovelluksen työkuormaan on kohdistettu kiinteä määrä muistia, prosessoria, levytilaa sovelluksen kysynnän tyydyttämiseksi. Tällainen staattinen lähestymistapa voi johtaa huomattavaan resurssien ylitarjontaan ja siten vaarana on, että resurssikustannukset ovat korkeammat pilvipalvelussa kuin perinteisessä konesalissa.

Edistyneempi lähestymistapa resurssienhallinnan näkökulmasta tukevat dynaamista aikaikkunaa. Virtuaalipalvelinten suhteen siten, että asiakas vain maksaa vain siitä mitä tarvitaan. Tämän mallin avulla asiakkaat voivat hallita tämän tyyppisiä kustannuksia lisäämällä tai vapauttaen virtuaalipalvelimen resursseja tarpeen mukaan.

Myös Chen, Y., Sion, R. (2014) viittaavat tähän, että pilvipalvelut ovat kustannustehokkaita, mikäli pilvikapasiteettiin liittyviä mekanismeja ei ole ulkoistettu kolmannelle osapuolelle. Tällainen osaamistyhjiö saattaa syntyä organisaatiossa, jossa on ollut kyvykkyyttä tuottaa palveluita omassa paikallisessa konesalissaan, mutta kun kapasiteetti ulkoistetaan pilveen, niin osaaminen joudutaan ostamaan ulkopuolelta.

Forbesin mukaan yritykset siirtyvät pilvipalveluihin halutakseen parantaa tehokkuutta, sekä tehdä kustannussäästöjä. Tämän hetken johtavat pilvipalveluidentarjoajat ovat

Amazon, Google ja Microsoft. Palveluntarjoajat voivat tarjota laajasti pilvipalvelutuotteita, kuten palveluja ja sovelluksia. Yritykset näkevät pilvipalveluiden tuovan säästöä päälaiteinvestoinneista,

sekä konesalikustannuksista. Nämä asiat ovat pääasiallinen syy siirtyä pilvipalveluun. Pitää huomioida, että pilvipalveluun siirtyessä yrityksellä on monia jo huomioitavia asioita. IT-resurssit, osaaminen sekä palveluntarjoajan valinta. (Forbes 2017.)

Organisaatiot siirtyvät hitaasti pilvipalveluihin koska on epäselvää, miten säästöjä saadaan aikaiseksi. Puhetta pilvipalveluista on paljon, mutta vielä ei ole löydetty kaikkia vahvuuksia, jotta yritykset ottaisivat palvelun käyttöön laajasti. Vaikka perinteiset IT-ratkaisut ovat kalliimpia kuin pilvipalvelut, operatiiviset kustannukset ovat silti korkeat. Pilvipalvelun tärkeimmät ominaisuudet tulevat skaalautuvuudesta, sekä resurssien käytöstä. Kapasiteettia voidaan näin ollen käyttää tarpeen ja tilanteen mukaan. Palveluita ja sovelluksia voidaan jakaa yksinkertaisemmin yrityksen sisällä. Laskutusmalli on yrityksille sopiva, jossa maksetaan käytön mukaan (The financial case for moving to the cloud 2017.)

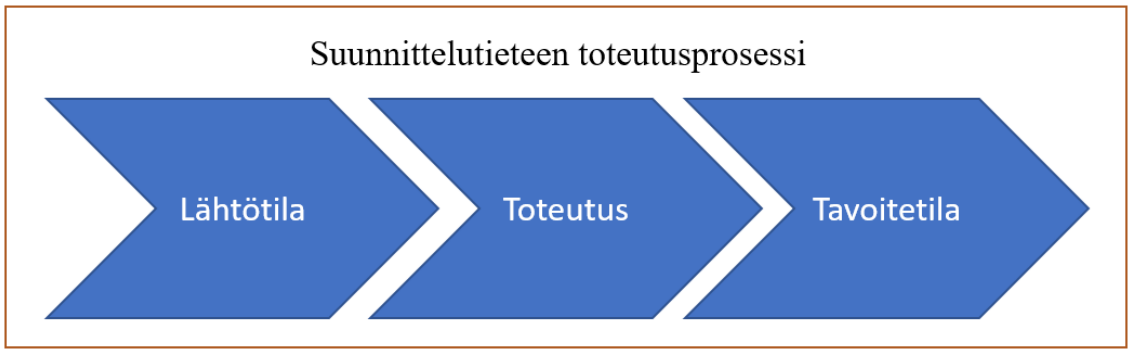
3 TUTKIMUSMENETELMÄT

Tämän Pro Gradu tutkimuksen yhtenä ominaispiirteenä on yksittäinen tapaus ja kohteena on organisaatio. Tässä työssä on kyse tämän yksittäisen tapauksen prosesseista ja ne ovat näin ollen kiinnostuksen kohteena. Näin ollen tutkimusta voidaan pitää tapaustutkimuksena (case-tutkimus). Tyypillistä tapaustutkimuksessa on tutkia yksityiskohtaista tietoa suurennuslasilla (Hirsijärvi ym. 2009: 134).

Tutkimuksessa verrataan perinteisiä konesaliratkaisuja pilvissä toteutettaviin vastaaviin tai edistyneimpiin ratkaisuihin, jolloin tästä syntyy myös vertaileva tutkimus. Ja koska tästä tapauksesta on kokemusperäistä syntynyttä tietoa ja sitä voidaan kuvata kokonaisvaltaisesti, sekä voidaan myös peilata teoriaan. Näin muodostuu myös kolmas näkökulma, kvalitatiivinen tutkimus (Hirsijärvi ym. 2009: 161).

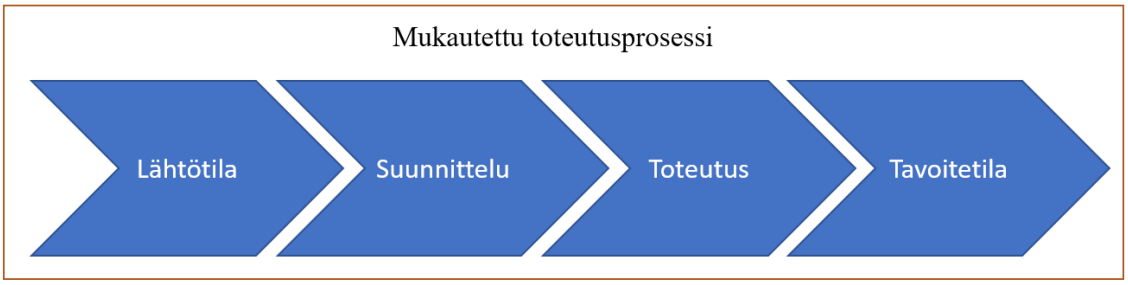
- Tiedonhakua kokonaisvaltaisesti ja tuloksia voidaan kerätä todellisista tilanteista
- Tutkimuksen tekijän omat havainnot, jotka vahvistavat käsitystä tutkimuksen kohteena olevasta yksittäisestä tapahtumasta
- Käytetään haastatteluita, dokumentteja ja havainnointia tutkimusmenetelminä. Tässä työssä käytetään näistä yllämainituista havainnointia, tieteellisiä sekä organisaation omia dokumentteja, joita on syntynyt pilvipalvelujen käyttöönoton yhteydessä
- Tutkimuksessa tulee esille eri näkökulmat tutkittavista kohteista, mm. kirjallisuus, havainnot (Hirsjärvi ym. 2009: 164).

Toisena tutkimusmenetelmän viitekehyksessä on suunnittelutiede (design science). Tässä tutkimuksessa on tarkoitus saada aikaan pysyvä muutos, jossa on alku – ja lähtötila. Siitä seuraa toteutusvaihe sekä tavoitetila (Järvinen & Järvinen 2011: 103). KEHA-keskus siirtyy käyttämään perinteisten konesalien rinnalla pilvipalveluita eli on luomassa jotain uutta vanhan rinnalle ja korvaa vanhan osittain.



Kuva 4. Suunnittelutieteen toteutusprosessi (Järvinen & Järvinen 2011: 103).

Yllä oleva kuvio on selkeä kuvaus siitä, miten suunnittelutieteen prosessi etenee. Tätä mallia hyödynnettiin tässä tutkimuksessa soveltavasti, jossa selvitettiin lähtötilanne, tarpeet ja mahdolliset saatavat hyödyt. Pilvitoteutuksen suunnittelussa (Kuva 5.) kartoitettiin eri pilvipalvelujen tuottamisvaihtoehtoja ja tehtiin ratkaisu siitä millä palveluntarjoajan vaihtoehdolla tämä työ lähdetään toteuttamaan. Toteutuksen osuus koostuu siitä mitä palveluita, järjestelmiä ja työkuormia on mahdollisuus siirtää mahdollisimman ketterästi ja kustannustehokkaasti pilvipalveluun. Tavoitetilassa tarkastellaan tuotettua toteutusta ja arvioidaan siitä saatuja suoranaisia hyötyjä.



Kuva 5. KEHA Pilvipalvelujen toteutusprosessi.

Kuten alkukappaleissa mainittiin, niin tutkittavana ilmiönä on KEHA-keskus organisaation siirtyminen pilvipalvelujen käyttäjäksi, josta tulee lisäarvoa tuotettavien palvelujen osalta kustannustehokkuuden, ketteryyden ja tietosuojan näkökulmasta.

Tutkielma toteutetaan myös osittain kirjallisuuskatsauksena. Lähteistä yritetään löytää tietoa pilvipalvelujen kustannustehokkuudesta, ketteryydestä sekä tietoturvasta. Tätä aineistoa peilataan ja verrataan case-yrityksen pilvipalvelun toiminnan kuvaamiseen ja ymmärtämiseen (Woodside 2010: 1).

Työssä käytetään laajalti Tritonian Finna- portaalin tarjoamaa aineistoa. Aineistoa on tarjolla laajasti pilvipalveluihin liittyen. Artikkeleita, E-kirjoja, tietokantoja: Ellibs, Elib, Ebook Central, ebooks on EBSCOhost, MyLibrary.

Hakukoneista eniten käytetty on Google schoolar, sekä Microsoftin tarjoamia artikkeleita pilvipalvelujen rakentamisesta hyödynnetään voimakkaasti. Niin tässä opinnäytetyössä, kuin itse ympäristön rakentamisessa.

4 PILVIPALVELUIDEN KÄYTTÖÖNOTTO- JA PALVELUMALLIT

Pilvipalvelujen käyttöönotto- ja palvelumallit käydään tässä luvussa läpi pääpiirteittäin. Niiden syvällisempi teoreettinen tarkastelu ei ole tässä työssä tarkoituksenmukaista, koska niistä löytyy jo valtavasti tietoa muista vastaavista tutkimuksista ja opinnäytetöistä. Liiketoiminnan näkökulmasta pilvipalvelut ovat palvelukeskeisiä. Käyttöönottomallit kuvaavat sitä kuka pilvipalvelua tarjoaa ja minkälainen organisaatio sitä käyttää. Palvelumallit taas kuvaavat vastuunjakoa pilvipalvelukomponentin operatiivisen hallinnan ja vastuun eri tasoista.

Pilvi-infrastruktuuri käsitettä on syytä avata tässä osiossa, sillä käsitteenä se ilmenee tässä työssä useasti. Pilvi-infrastruktuuri on laitteiston ja ohjelmiston kokoelma, joka mahdollistaa pilven viisi olennaista ominaisuutta tietojenkäsittelyssä. Pilvi-infrastruktuuri pitää sisällään sekä fyysisen kerroksen, että abstraktiivisen kerroksen.

Fyysinen kerros koostuu laitteistoresursseista, jotka ovat välttämättömiä tarjottavien pilvipalvelujen tukemiseksi, ja tyypillisesti sisältyy palvelin-, tallennuskapasiteetti- ja verkkokomponentit. Abstraktiokerros koostuu fyysisen kerroksen kautta asennetusta ohjelmistosta, joka ilmentää olennaisia pilvien ominaisuuksia. Käsitteellisesti abstraktiokerros sijoittuu fyysisen kerroksen yläpuolelle (NIST 2011 :3).

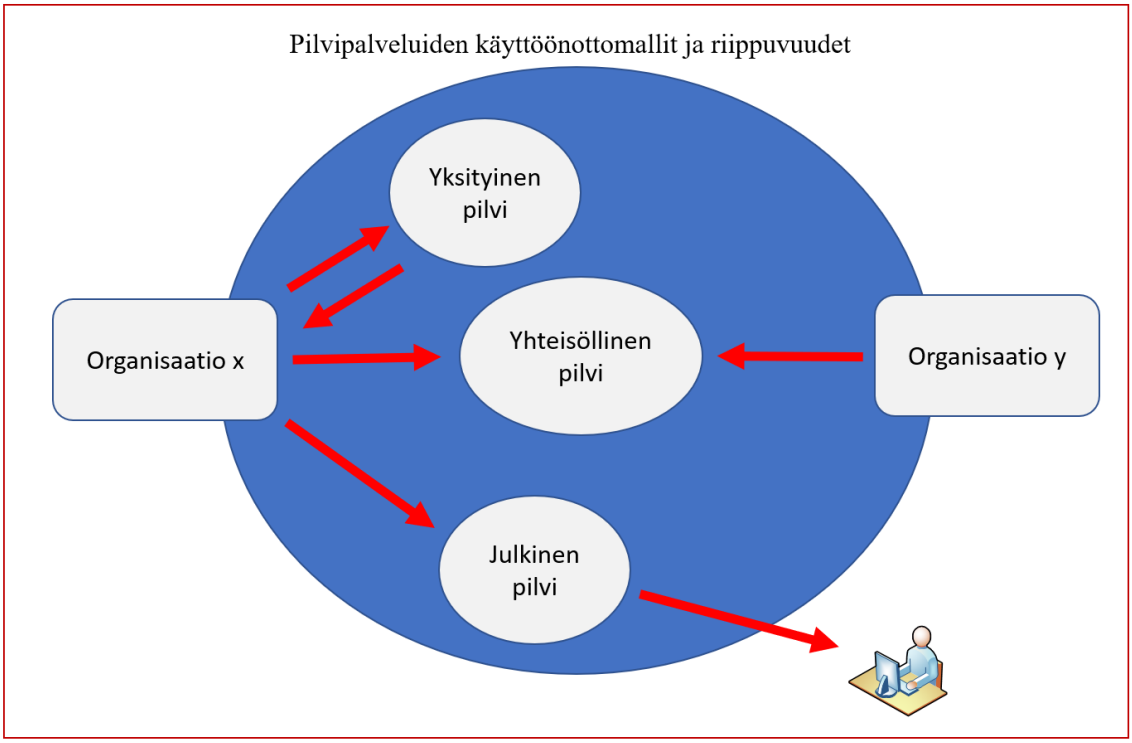
4.1 Yleisimmät käyttöönottomallit

Julkinen pilvi on yleisin pilvipalvelun käyttöönottomalli. Tässä mallissa palveluntarjoaja tarjoaa palveluita isolle käyttäjämassalle. Tässä mallissa palvelun käytöllä on tietyt pelisäännöt ja ne eivät luonnollisesti ole räätälöitävissä asiakaskohtaisiksi. Pilvi-infrastruktuuria tarjotaan suurelle yleisölle avoimesti ja tyypillisesti sitä hallinnoi yritys, akateeminen tai julkishallinnon organisaatio tai jokin näiden yhdistelmä. Tyypillisesti se on kaupallisen pilvipalvelutoimittajan tuottama palvelu (NIST 2011: 3).

Yksityinen pilvi. Pilvi-infrastruktuuri on varattu yksinomaiseen käyttöön yhdelle organisaatiolle, joka koostuu useista kuluttajista (esim. liiketoimintayksiköistä). Se voi olla organisaation omistama, hallinnoima pilvi-infrastruktuuri. Ja sen ylläpito toimeenpannaan tyypillisesti organisaation ja/tai kolmannen osapuolen toimesta. Yksityinen pilvi voi olla toteutettuna perinteisessä konesalissa tai kaupallisen toimijan pilvipalvelussa (NIST 2011: 3).

Yhteisöllinen pilvi. Pilvi-infrastruktuuri on varattu ja jaettu yhden tai useamman organisaation kesken. Tyypillisesti tällainen tilanne syntyy, kun organisaatioilla on samat intressit koskien turvallisuusvaatimuksia, käytäntöjä tai muuta sellaista, jonka synergiasta on hyötyä molemmille tai useammalle organisaatiolle. Tyypillisesti sitä hallinnoi organisaatiot yhdessä sekä kolmannen osapuolen avulla. Tyypillisiä teknisiä ratkaisuja voi olla perinteinen konesali tai kaupallisen pilvipalvelutoimittajan tiloissa (NIST 2011: 3).

Hybridipilvi. Pilven infrastruktuuri koostuu kahdesta tai useammasta erillisestä pilvestä tai siinä on ominaisuuksia useammasta eri pilvipalvelumallista. Pilvi-infrastruktuurit (yksityiset, yhteisölliset tai julkiset) ovat omia kokonaisuuksia, mutta ne voidaan yhdistää käyttämällä standardoituja yhdyskäytäväratkaisuja, joka mahdollistaa datan ja sovellusten liikenteen eri pilvipalvelumallien välillä. Hybridipilven suunnittelu ja toteutus on vaativampaa kuin yksittäisen pilvipalvelumallin käyttöönottaminen (NIST 2011: 3).



Kuva 6. Pilvipalveluiden käyttöönottomallit ja riippuvuudet (NIST 2011: 2).

Kuviossa 6 kuvataan eri käyttöönottomalleja ja niiden riippuvaisuuksia. Organisaatio, joka käyttää yksityistä pilveä ja ei tarjoa sitä muille organisaatiolle tai kansalaisille, niin silloin sitä kutsua yksityiseksi pilveksi. Organisaatio, joka jakaa pilvi-infrastruktuurin toisen organisaation kanssa, voidaan puhua yhteisöllisestä pilvestä. Julkinen pilvi voi olla esimerkiksi organisaation, joka tuottaa sovelluksen kansalaiselle, mutta käyttää sitä myös itse tai se voi olla puhtaasti kansalaiselle suunnattu palvelu.

4.2 Yleisimmät pilvipalvelumallit

Ohjelmisto palveluna (SaaS). Kuluttajalle tai organisaatiolla on mahdollisuus käyttää palveluntarjoajan sovelluksia, jotka toimivat palveluntarjoajan pilvi-infrastruktuurissa. Tyypillisesti sovellukset ovat saatavilla ja käytettävissä erilaisilla asiakas – ja päätelaitteilla. Niitä käytetään pääasiassa internet-selaimella tai sovelluksen käyttöliittymällä. Esimerkkinä selaimella käytettävä sähköposti (webmail) on tyypillinen SaaS-sovellus.

Kuluttajalla ei mahdollisuutta hallita, eikä ohjata SaaS-pohjaista pilvi-infrastruktuuria, mukaan lukien verkot, palvelimet, käyttöjärjestelmät ja levyjärjestelmä. Yksilöllisiä sovellusominaisuuksia ei juurikaan voida muokata, lukuun ottamatta rajoitettuja käyttäjäspesifisiä sovelluksen kokoonpanoasetuksia tai muita personointiasetuksia (NIST 2011: 3).

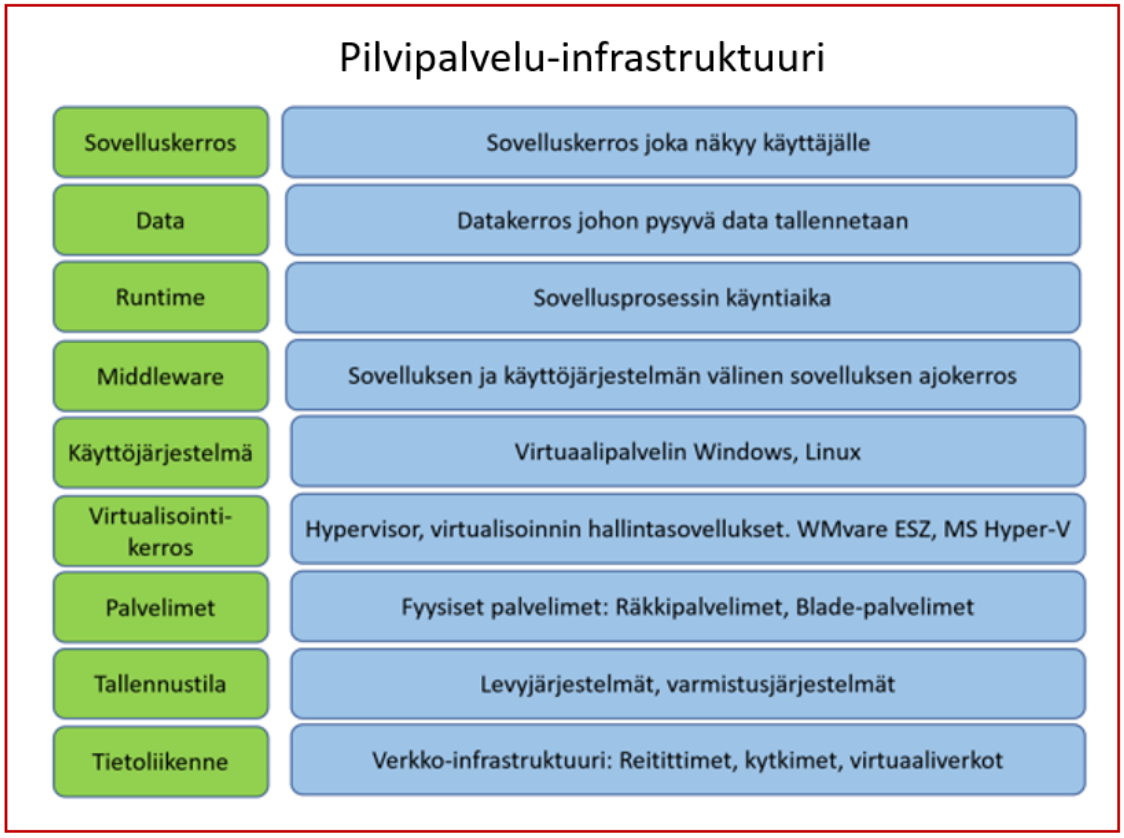
Sovellusalusta palveluna (PaaS). Kuluttajalle tai organisaatiolle mahdollistetaan kyky ottaa käyttöön pilvi-infrastruktuurissa hankittuja sovelluksia, joita voidaan räätälöidä ohjelmoinnin avulla ja käyttämällä sellaisia ohjelmointikieliä, kirjastoja, palveluita ja työkaluja, joita palveluntarjoaja tukee.

Kuluttaja tai organisaatio ei hallitse taustalla olevaa pilvi-infrastruktuuria, kuten verkkoja, palvelimia, käyttöjärjestelmiä tai tallennustilaa, mutta se hallitsee sovelluksia ja mahdollisesti sovelluksen ylläpitoympäristön kokoonpanoasetuksia (NIST 2011: 3).

Infrastruktuuri palveluna (IaaS). Kuluttajalle tai organisaatiolle tarjotaan kyky provisioida käsittely-, tallennus-, verkko- ja muut keskeiset tietojenkäsittelyresurssit, joissa kuluttaja tahi organisaatio pystyy ottamaan käyttöön ja käyttämään mitä tahansa ohjelmistoa, johon voi kuulua käyttöjärjestelmäosio ja sovellusosio. Tyypillisesti tällainen IaaS-komponentti on virtuaalinen palvelin (Virtual Machine) käyttöjärjestelmällä varustettuna.

Kuluttaja tai organisaatio ei hallitse palvelutarjoajan pilvi-infrastruktuuria, mutta se hallitsee käyttöjärjestelmä-, tallennuskapasiteetti- ja verkkokerrosta sekä virtuaalipalvelimessa olevia sovelluksia. Kuluttaja tai organisaatio hallitsee verkko-osuudesta vain sen

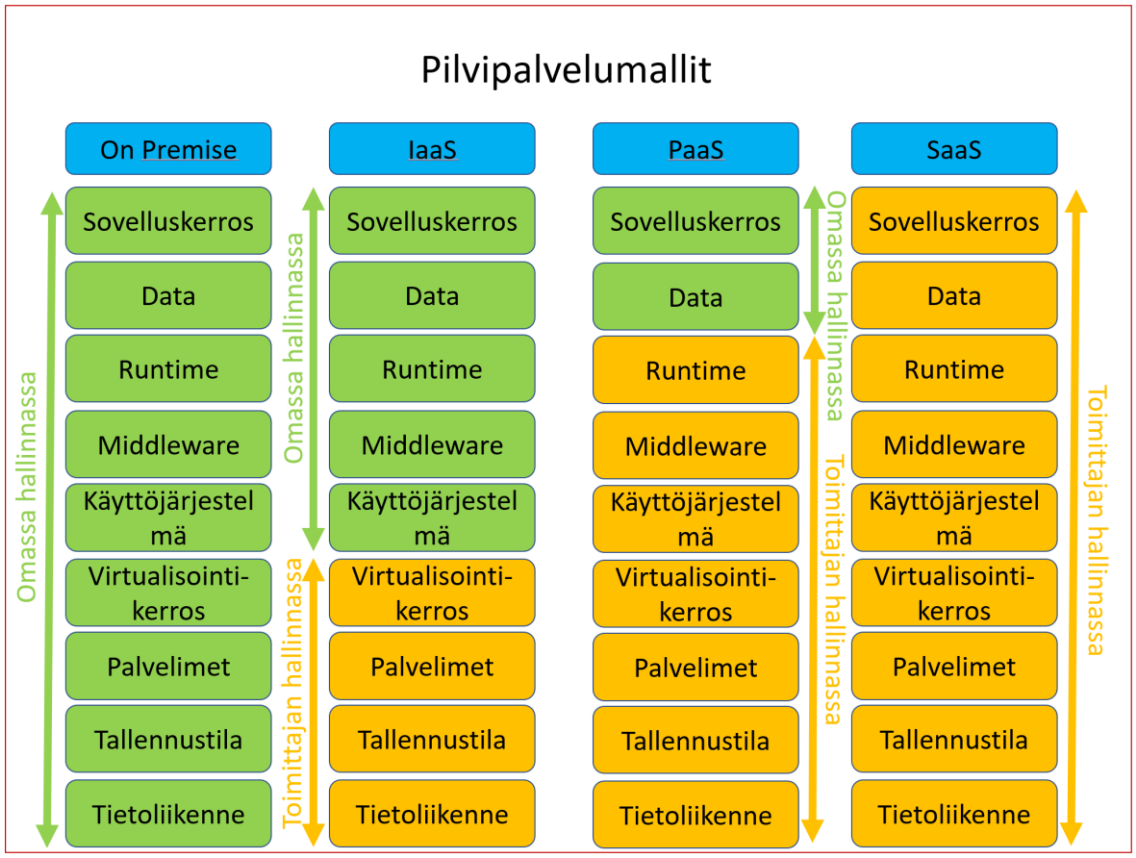
loogisen osion, joka hänelle on osoitettu palveluntarjoajan provisioinnissa, sekä siihen kohdistetut peruspalomuuritoiminnallisuudet (NIST 2011: 3).



Kuva 7. Pilvipalvelu-infrastruktuurin eri kerrokset.

Pilvipalvelun infrastruktuuria voidaan kuvata monella eri tavoin. Tämä kerroskuva (Kuva 7.) on yleisin tapa kuvata pilvipalvelun infrastruktuuria, josta löytyy monta eri versiota, miten ja mitä asioita halutaan tuoda ja painottaa kuvassa. Toisessa kuvassa (Kuva 8.) esitetään pilvi-infrastruktuurin eri vastuualueita riippuen siitä mikä malleista on käytössä. On-Premise, IaaS, PaaS tai Saas, jossa On-Premisenä tuotettu palvelu on täysin organisaation hallitsema konesalin hallinnasta lähtien aina sovelluksen tuottamiseen asti.

IaaS -malli tarjoaa käyttäjäorganisaatiolle valmiin virtuaalipalvelimen perusasetuksilla, jossa on käyttöjärjestelmä valmiina. Toimittajan vastuulle jää virtualisointialustat, fyysiset palvelinraudat, sähkönsyöttö, jäähdytys, toimitilan fyysinen turvallisuus sekä toimitilan omistamisesta tai vuokraamisesta aiheutuvat muut kulut.



Kuva 8. Pilvipalvelun palvelumallit.

Kuvan 8. vasemmassa laidassa On-premise kuvaa sitä tilannetta, jossa asiakas ylläpitää ja vastaa kaikista infrastruktuurikerroksista. Pilvipalvelun tarjoama IaaS-ratkaisussa asiakas vastaa käyttöjärjestelmäkerroksesta ja sen päälle rakennettavasta sovelluskerroksesta. PaaS-ratkaisussa palveluntarjoaja hoitaa myös käyttöjärjestelmäkerroksen, jolloin asiakkaan vastuulle jää sovelluskerroksen rakentaminen ja ylläpito. SaaS-palvelussa palvelun-

tarjoaja vastaa myös sovelluskerroksesta, jolloin asiakkaan vastuulle jää vain itse sovelluksen sisällöntuotannosta. Esimerkkinä voidaan mainita Microsoftin tarjoama Office 365-palvelu.

5 CASE: KEHA-KESKUS TIETOJÄRJESTELMÄT SUUNNITTELU

Tässä kappaleessa on tarkoitus käydä lävitse Microsoft Azure käsitteistöä ja Microsoft filosofiaa ja toimintatapoja sekä miten pilvipalvelut tulisi rakentaa. Kappaleessa käydään läpi KEHA-keskuksen tietojärjestelmätuotannon nykytilaa sekä keskitytään erityisesti teknisen tietoturvan toteuttamiseen.

5.1 Keskeiset Microsoft Azure- käsitteet

Keskeiset käsitteet tässä työssä ovat lähinnä IT-alalla yleisiä käytössä olevia käsitteitä. Tässä tutkielmassa pilvipalvelua koskevat käsitteet pohjautuvat pitkälti Microsoft Azure pilvipalveluun, vaikkakin samoja käsitteitä käytetään muissakin pilvipalvelutarjoajien ympäristöissä, niistä vain puhutaan joissain tapauksissa hivenen eri termein. Näistä edellä mainituista syistä Microsoft Azurea koskevat käsitteet on syytä avata tarkemmin tässä tutkielmassa. Taulukossa 1. esitetään Azure käsitteistöä.

Taulukko 1. Azure käsitteistö

Account	Organisaation Azure tili, joka toimii laskutus -ja asiakastie-tojen pohjana
App Service	Sovellus palveluna (PaaS)
App Service plan	Määritellään sovelluspalveluun liittyviä kyvykkyyksiä
Back-End	Eriytetty looginen virtuaaliverkko tietokantaalustoille
Load Balance (LB)	Tietoliikenteen kuormantasaus
Front-End	Eriytetty looginen virtuaaliverkko internet- rajapinnassa
Gateway	Tietoliikenteen yhdyskäytävä
Inbound	Sisäänpäin suuntautuva tietoliikenne
Mid-Tier	Eriytetty looginen virtuaaliverkko sovellusalustoille

Network interface (NIC)	Verkkorajapinta/Virtuaalinen verkkokortti, joka tyypillisesti kytketään virtuaaliseen palvelimeen
NSG	Network Security Group, Azuren tarjoama palomuuripalvelu, joka sisältää palomuurille tyypilliset perustoiminnallisuudet
Outbound	Ulospäin suuntautuva tietoliikenne
Public IP address (PIP)	Julkinen verkko-osoite, joka kytketään verkkorajapinnassa olevaan virtuaaliseen verkkokorttiin.
Resource Group (RG)	Resurssiryhmä, johon voidaan linkittää eri resursseja samaan ympäristöön.
Storage Account (SA)	Tallennuskapasiteetti, joka allokoidaan virtuaaliselle palvelimelle
Subnet	Aliverkko, joita voidaan määritellä useita yhteen virtuaaliseen verkkoon (VNet)
Subscription	Azure pilvitili, joita voi olla useampia yhdellä organisaatiolla
Virtual Machine (VM)	Virtuaalinen palvelin, IaaS
Virtual Network (VNet)	Virtuaalinen verkko, johon voidaan liittää useita aliverkkoja (Subnet)
Virtual Network GW	Virtuaalinen verkkoyhdyskäytävä VPN-yhteyksiä varten

5.2 KEHA-keskus On-Premise -konesalipalvelut

KEHA-keskus on tarjonnut valtionhallinon asiakkaille tietojärjestelmäpalveluita vuodesta 2009. KEHA-keskuksen tehtävänä on tuottaa ja kehittää sähköisiä palveluita ELY-keskuksille, TE-Palveluille, Aluehallintovirastolle (AVI), Maistraateille sekä muille valtiohallinnon virastoille. KEHA-keskus tunnettiin aiemmin Aluehallinnon tietopalvelu – yksikkönä vuosina 2009-2014.

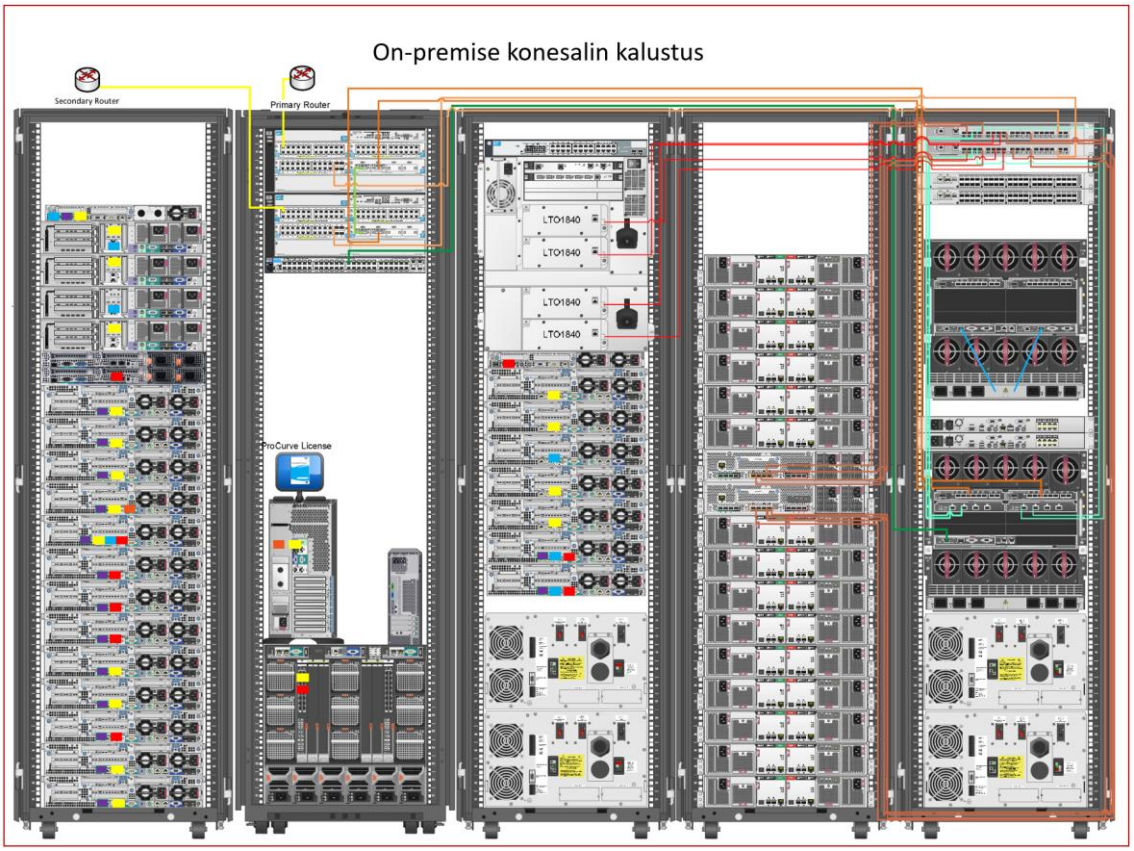
Edellisen aluehallintouudistuksen myötä (v.2008) omien konesalien ja palveluiden konsolidoinnin tarve ELY-keskukselle, AVI:lle, Maistraateille ja TE-palveluille oli suuri. Tavoitteena oli perustaa kaksi konesalia eri paikkakunnille, mutta identtisellä palvelinkalustuksella, josta tulisi synergia- ja hallintaetuja jatkuvien palvelujen osalta.

Konesalit ovat virastotalon laitetiloiksi tarkoitetuissa tiloissa. Tilat ovat vuokratut ja niistä maksetaan kuukausittaista vuokraa, sekä luonnollisesti sähkönkulutuksesta ja jäähdytyksestä aiheutuvat kulut. Konesalien rakentamisesta aiheutuneet kulut, kuten korotettu lattia, palo- ja turvahälytysjärjestelmät ovat kustannuksien osalta vuokraajan vastuulla.

Nykyinen hallintamalli on moniportainen. Valtion tieto- ja viestintätekniikkakeskus Valtori on ollut konesalien omistaja vuodesta 2014 lähtien. KEHA-keskuksen ja Valtorin välillä on kapasiteettipalvelun osalta tilaaja -tuottaja malli. On-Premise -kapasiteetin toimitusketjua voisi yksinkertaisesti kuvata seuraavalla esimerkillä. Työ- ja elinkeinoministeriö (TEM) asettaa tietojärjestelmäprojektin. Projekti siirtyy KEHA-keskuksen projektitoimiston projektisalkkuun. Kun projekti käynnistyy, niin projektin alkuvaiheessa kuvataan järjestelmän tarpeet.

Lähes poikkeuksetta järjestelmästä tehdään testi – ja kehitysympäristö ennen tuotantoympäristön pystyttämistä. Projekti pystyy näin tilaamaan Valtorilta On-Premise -kapasiteettia mikäli se katsotaan aiheelliseksi. Esimerkiksi jos tietojärjestelmässä käsiteltävän tiedon luokittelu kuuluu suojaustaso III, niin silloin lähes poikkeuksetta järjestelmä tulee olla tuotettuna Suomessa ja siinä käsiteltävän datan tallennussijainti Suomessa.

Tätä ei kuitenkaan suoraan sanota missään Suomen Valtiolle suunnatuissa tietojenkäsittelyohjeissa, vaan siitä on tullut yleinen konsensus virastojen tietohallinnon tekemien tulkintojen perusteella Valtiovarainministeriön VAHTI-ohjeesta. Tietojenkäsittelyn yleiset tietoturvavaatimukset ja tiedon käsittelyn eri suojaustasot määritellään Valtionvarainministeriön VAHTI-ohjeessa (Valtiovarainministeriö, 2010).



Kuva 9. On-Premise konesalin kalustuskuva vuodelta 2010.

Kuvassa 9. esiintyy On-premise -konesalin kalustuskuva, jossa komponentit ovat sijoitettu neljään erilliseen laitekehikkoon. Äärivasemmalla olevassa kehikossa on räkkipalvelimet. Räkkipalvelin sisältää tyypillisesti kaikki palvelimen tarvitsemat komponentit. Emolevyn, prosessorit, muistit, verkkokortin sekä tallennuslevyn. Näillä komponenteilla palvelin kykenee tuottamaan itsenäisesti palveluja, kunhan se kytketään konesalin runkokytkimeen.

Runkokytkin on liitetty taas konesalireitittimeen, josta taas tietoliikenne lähtee ulos konesalista, joko ulkoverkkoon eli internettiin tai sitten liikenne ohjataan sisäverkkoon riippuen palvelusta mitä tuotetaan. Runkokytkimiä ja reitittimiä on kaksi kumpaakin. Reitittimet on konfiguroitu siten, että toinen reitittimistä on Primary eli pääreititin, jota pitkin liikenne kulkee pääsääntöisesti. Backup-reititin on varayhteyttä varten, mikäli pääreititin vikaantuu.

Reitittimissä käytetään Hot Standby Router Protokollaa (HSRP). Se on Ciscon kehittämä redundanssiprotokolla vikasietoisen oletusyhdyskäytävän luomiseksi. Protokolla muodostaa reitittimien välille virtuaalisen yhdyskäytävän. Mikäli toinen reitittimistä vikaantuu, niin yhdyskäytävä osaa siirtää liikenteen toiselle reitittimelle.

Teknisesti se tapahtuu siten, että ensisijainen reititin (Primary), jolla on korkein määritetty prioriteetti, toimii virtuaalisena reitittimenä ennalta määritetyllä yhdyskäytävä IP-osoitteella. Se reagoi ARP- tai ND-pyyntöön konesaliverkkoon kytketyistä palvelimista virtuaalisella MAC-osoitteella. Jos ensisijaisen reitittimen liikenteenvälitys epäonnistuu, reitittimen, jolla on seuraavaksi korkein prioriteetti (tässä tapauksessa Backup eli vararеititin), ottaa yhdyskäytävän IP-osoitteen ja vastaa ARP-pyyntöihin samalla MAC-osoitteella. Näin saadaan läpinäkyvä yhdyskäytävä riippumatta siitä, kumpi reititin on toiminnassa.

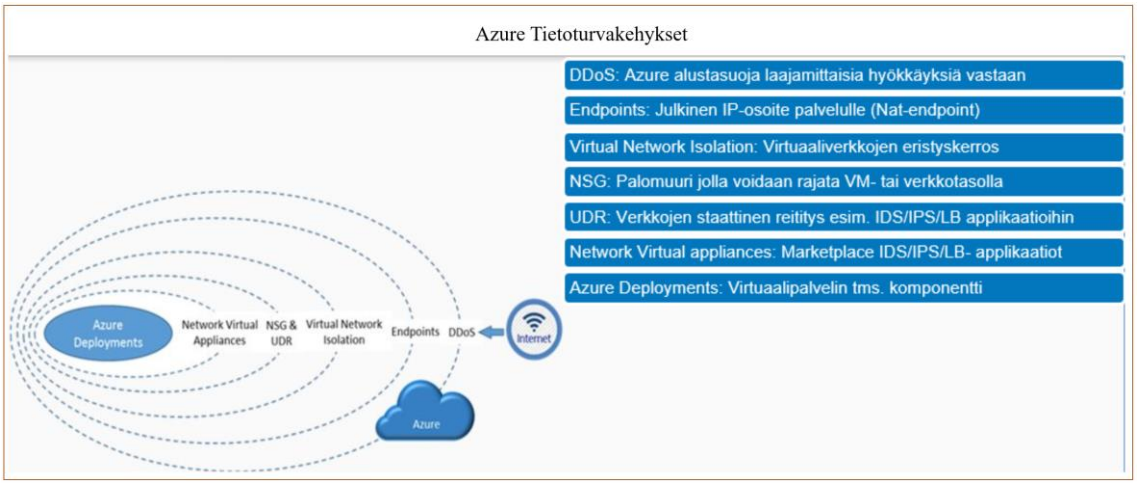
Primary-reititin on kytketty 1. runkokytkimeen. Backup-reititin on kytketty 2. kytkimeen. Runkokytkimet ovat yhteydessä toisiinsa 10GB kuitukaapelilla. Tällä tavoin saadaan vikasietoisuutta myös runkokytkinten osalta, mikäli toinen laitteista vikaantuu. Kuvassa 9. toisena vasemmalle olevan laitekehikon ylälaidassa on periaatekuva konesalin reitittimistä ja kytkimistä.

5.3 KEHA-keskus pilvipalvelut

Ketteryys ja kustannustehokkuus olivat ajureita, joista lähti liikkeelle KEHA-keskuksen pilvipalvelujen kokeilu. Kustannustehokkuus on tosiasia, joka pilvipalvelussa saavutetaan teoriatasolla. Kuitenkin yrityksiltä, jotka ovat siirtyneet käyttämään pilvipalveluita eivät ota kaikkea kustannuspotentiaalia irti mitä pilvipalveluilla on saatavissa.

Microsoftin pilvipalvelut tarjoavat tunnetusti skaalautuvia palveluita, skaalautuvaa pilvi-infrastruktuuria, yritystason ominaisuuksia ja monia vaihtoehtoja hybridisovelluksille. Asiakkaat voivat halutessaan käyttää näitä palveluja joko Internetin kautta tai Azure ExpressRouten avulla, joka tarjoaa yksityisen verkkoyhteyden.

Microsoft Azure -alustalla asiakkaat voivat laajentaa infrastruktuuriaan pilviin ja rakentaa monitasoisia arkkitehtuureja. Kolmannet osapuolet voivat lisäksi parantaa valmiuksia tarjoamalla turvallisuuspalveluja ja virtuaalisia laitteita.



Kuva 10. Azure tietoturvakehykset.

Vaikka pilvipalveluja tarjoavat yritykset panostavat voimakkaasti pilvi-infrastruktuurin suojaamiseen, asiakkaiden on myös suojeltava pilvipalveluitaan ja resurssiryhmiä. Monikerroksinen lähestymistapa turvallisuuteen tarjoaa parhaan puolustuksen. Perimetrinen verkkoturvallisuusvyöhyke suojaa sisäisiä verkkoresursseja epäluotetusta verkosta. Kehäverkko viittaa Internetin ja suojatun yrityksen IT-infrastruktuurin välisiin verkon reunoihin tai osiin. Kuvassa 10. esitetään monikerroksinen lähestymistapa pilven suojaamiseen.

Tyypillisissä yritysverkoissa perusinfrastruktuuri on voimakkaasti vahvistettu kehysperiaatteella, joissa on useita suojauskehyksiä ts. kerroksia. Näissä kerroksissa voidaan suojata infrastruktuuria erilaisin komponentein. Jokaisen kerroksen raja koostuu laitteista ja suojauspolitiikan valvontapisteistä. Jokainen kerros voi sisältää esimerkiksi seuraavien verkkoturvalaitteiden yhdistelmän: palomuurit, palvelunestohyökkäykset (DOS), Intrusion Detection- tai Protection Systems (IDS / IPS) ja VPN-laitteet. Politiikan valvonta voi olla palomuurisääntöjä, pääsynvalvontaluetteloita (ACL) tai tiettyä reititystä (UDR).

Verkon ensimmäinen puolustuslinja, joka vastaanottaa suoraan Internetin saapuvan liikenteen, on näiden mekanismien yhdistelmä estämään hyökkäykset ja haitallinen liikenne

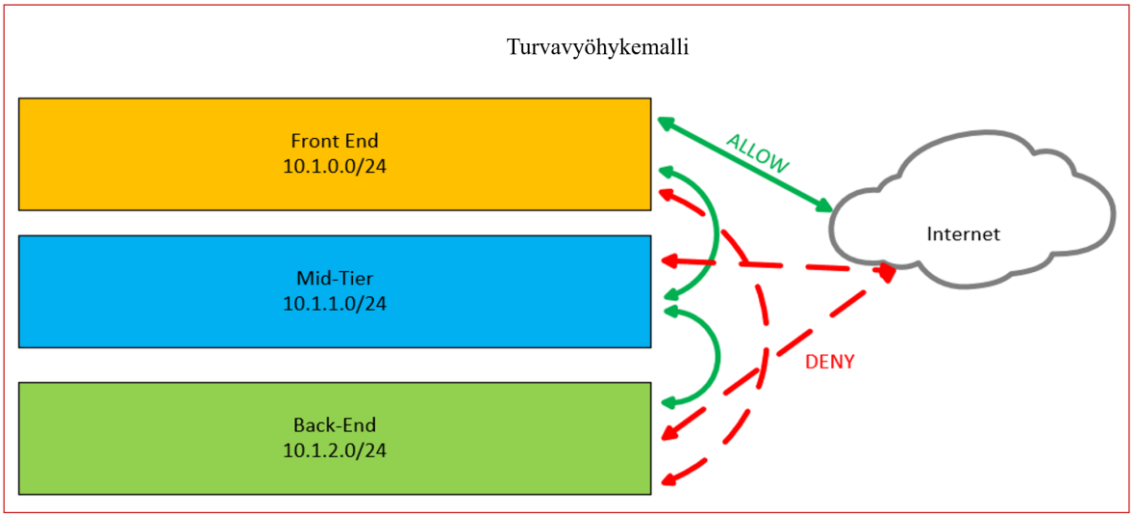
sallien oikeutetut pyynnöt edelleen verkkoon. Azuren alustasuojauksen uloin DDoS-kerros ei ole asiakkaan hallinnassa tai konfiguroitavissa ja se ei näy millään tavalla asiakkaan hallintaliittymässä.

Nämä liikenneväylät kulkevat suoraan kehäverkon resursseihin. Tämä resurssi voi sitten ”puhua” resursseille syvemmälle verkossa, jolloin seuraava validointiraja siirtyy ensin. Uloin kerros kutsutaan kehäverkoksi, koska tämä verkon osa altistuu Internetille, yleensä kummallakin puolella. Seuraavassa kuvassa on esimerkki yhdestä aliverkon kehäverkosta yritysverkossa, jossa on kaksi suojausrajaa.

5.4 Tietoturva

Tässä työssä keskitytään pilvipalvelun teknisen tietoturvan parantamiseen ja toteutukseen. Lähtökohtana on se, että pilvipalvelu on saatava minimissään samalle teknisen tietoturva tasolle kuin olemassa oleva On-Premise-infrastruktuuri. Tässä työssä ei syvemmin käsitellä hallinnollista tietoturvaa eikä organisaation tietosuojakäytäntöjä, jotka yhdessä teknisen tietoturvan kanssa muodostuvat yhdeksi kokonaisuudeksi organisaatiossa.

Lähtökohdaksi suunnittelussa KEHA-pilvipalvelun tietoliikenneverkon teknisen tietoturvan osalta kartoitettiin turvavyöhyke-mallia (Security Zone Model). Se on suhteellisen tehokas strategia erilaisten riskien vähentämiseksi ja on suhteellisen yksinkertainen toteuttaa tässä skenaariossa. Lisäksi se on kustannustehokas tapa toteuttaa teknistä tietoturvaa, koska perusratkaisussa ei tarvita kolmannen osapuolen tietoturvatuotetta pilviympäristössä. Kuvassa 11. esitetään verkkosegmentointi, joka on suositeltu tapa toteuttaa segmentointi pilvessä.



Kuva 11. KEHA-keskus Security Zone Model.

Lähtökohtana turvavyöhykemallissa on se, että internettiin päin suuntautuva eli pilvikonesalista ulospäin (outbound) suuntautuva liikenne on sallittu vain edustaverkosta (Front End).

Samanlainen periaate on myös sisäänpäin (Inbound) liikenteen osalta, jossa internetistä sisäänpäin suuntautuva liikenne on sallittu vain edustaverkko-segmenttiin. Tämä on kuvattu vihrein nuolin kuvassa 11.

Edustaverkosta voidaan liikennöidä internetin lisäksi vain keskimmäiseen verkkokerrokseen (Mid-Tier). Edustaverkoista taas ei voida liikennöidä suoraan taustaverkkosegmenttiin (Back-End). Kielletty liikennöintisuunta esitetään kuvassa 11. punaisilla nuolilla.

Keskimmäisestä verkkokerroksesta voidaan liikennöidä edustaverkkoon sekä taustaverkkoon. Mutta liikennöinti suoraan internettiin ei ole sallittua kumpaankaan liikennöintisuuntaan (Inbound / Outbound). Taustaverkosta voidaan liikennöidä vain keskimmäiseen verkkokerrokseen. Siitä ei saa olla muita yhteyksiä edustaverkkoon eikä internetin suuntaan.

Segmentointi erottaa järjestelmien vastuualueita ja hallitsee näiden välisiä riippuvaisuuksia. Jokaisella kerroksella on erityinen vastuu. Korkeampi verkkokerros voi tyypillisesti kutsua palvelua alemmasta kerroksessa, mutta tyypillisesti ei toisinpäin.

Pilvessä verkkokerrokset ovat loogisesti erillään, ja siellä toimivat palvelut rakennetaan erilaisin virtuaalipalvelimin. Tyypillisesti ylempi taso ottaa yhteyttä toiseen tasoon suoraan tai käyttää asynkronista viestinvälitystä (viestijonoa).

Verkkosegmenttien looginen erottaminen parantaa skaalautuvuutta ja joustavuutta, mutta lisää myös latenssia (viive) ylimääräisestä verkkoviestinnästä. Tosin latenssiongelmaa ei juurikaan pääse syntymään, mikäli puhutaan yhden keskitetyn datacenterin pilvipalveluympäristöstä. Verkkosegmenttien hajauttamiseen fyysisesti eri pilvikonesaleihin ei ole tältä osin ole perusteltua. Se pikemminkin toisi latenssista johtuvia haittavaikutuksia järjestelmän käytön aikana ja näkyy loppuasiakkaalle palvelun hitaudessa, jos sovelluksen ja tietokannan välinen latenssi on suuri. Perinteisellä kolmiportaisella sovelluksella on esitys-, sovellus- ja tietokantakerros.

Tämän tyyppinen sovellusarkkitehtuuri voidaan toteuttaa joko suljetun kerroksen arkkitehtuurilla tai avoimella kerrosarkkitehtuurilla. Suljetun kerroksen arkkitehtuurissa verkkosegmentti voi liikennöidä vain yhden segmentin alaspäin. Avoimessa kerrosarkkitehtuurissa mikä tahansa verkkosegmentti voi liikennöidä minkä tahansa kerroksen kanssa. Suljetun kerroksen arkkitehtuuri rajoittaa kerrosten välisiä riippuvuuksia. Se voi kuitenkin luoda tarpeetonta verkkoliikennettä, jos yksi kerros siirtää pyyntöjä seuraavalle kerrokselle.

Verkkosegmentoitu arkkitehtuuri sopii tyypillisesti infrastruktuuri palveluna (IaaS) -ratkaisuissa, jossa kullakin tasolla ajetaan erillisiä virtuaalipalvelimia. Tässä mallissa järjestelmän ei kuitenkaan tarvitse olla puhdas IaaS -ratkaisu. Usein on edullista käyttää PaaS-palveluja joillekin arkkitehtuurin osille, esimerkiksi palvelun julkaisukerrokselle, jossa palvelun ruuhka-aikana saadaan ketterästi ja kustannustehokkaasti skaalautuvuutta. Tiedon tallennus voidaan myös PaaS -tietokanta ratkaisujen avulla.

Verkkosegmentteihin perustuva arkkitehtuuri sopii hyvin yksinkertaisiin web-sovelluksiin. Se soveltuu myös On-Premise-ympäristöissä ajettavien sovellusten migraatioita pilvikonesaliin, mikäli arkkitehtuuri noudattaa samoja periaatteita. Tämä mahdollistaa vähäisen muutoskonfiguraation sovellusten osalta. Yhtenä etuna voidaan pitää myös sovellusten arkkitehtuuria, jossa sovelluksen sijainnilla ei ole väliä, vaan sovellusarkkitehtuurin näkökulmasta toiminnallisesti on sama, sijaitseeko sovellus On-Premise- vai Pilvipalveluympäristössä.

Mikäli verkkosegmentoitua ratkaisua on käytetty On-Premise- ympäristöissä, on niissä ajettavien työkuormien siirtäminen pilvipalveluun luonnollista ja ei vaadi isoja muutoksia järjestelmäkonfiguraatioon tai arkkitehtuuriin.

Mikäli pilvipalveluun on toteutettu testi-, kehitys- ja tuotantoympäristöt mainitulla verkkoarkkitehtuurilla on sovellustensiirrettävyys ja yhteensovitus luonnollista näiden välillä. Sovelluskehittäjän näkökulmasta tässä mallissa on vähemmän oppimiskäyrää ja on luonnollinen evoluutio perinteisestä sovellusmallista. Ajettavat ympäristöt ovat myös heterogeenisiä Windows- tai Linux -käyttöjärjestelmiä, jotka ovat tuttuja useimmille sovelluskehittäjille.

Haasteena voidaan vanhoja tietojärjestelmiä, joissa ei ole otettu huomioon segmentointia. Verkkosegmentoinnin monoliittinen rakenne saattaa hankaloittaa uuden komponentin tai ominaisuuksien itsenäisen käyttöönoton. Myös IaaS- virtuaalipalvelimella toimiva sovelluksen hallinta on työläämpää kuin PaaS- teknologialla toteutettu palvelu, jossa ylläpitäjän vastuulla jatkuvien palvelujen osalta on vain itse sovelluskerros. Vaikka segmentointi tuo turvaa tekniselä tasolla, niin sitä voi olla vaikea hallita suuressa pilviympäristössä, jossa on useita järjestelmiä.

6 CASE: KEHA-KESKUS TIETOJÄRJESTELMÄT TOTEUTUS

Toteutusta lähdettiin tekemään esiselvityksen perusteella ja työssä käytettiin Microsoftin konsultaatiota niiltä osin kuin katsottiin tarpeelliseksi. Ennen työn alkamista oli jo syntynyt käsitys siitä, että työssä tulisi pitäytyä Microsoftin parhaiden käytäntöjen mukaisissa ratkaisuissa.

6.1 KEHA-keskus konesalipalvelut

KEHA-keskuksen konesalipalvelut ovat aiemmin olleet perinteisesti tuotettuja tietojärjestelmäpalveluita. Ne ovat sijainneet joko omissa palvelinsaleissa tai toimittajan palvelinsalissa. Pilviteknologioista puhuttaessa törmää usein sanaan hybridi. Hybriditoteutus yleensä mielletään sellaiseksi, jossa yhdistetään uutta ja vanhaa teknologiaa. Myös tässä tapauksessa voidaan puhua hybridiratkaisusta pääosin. Tietojärjestelmän kehityksen kannalta, itse tietojärjestelmät ovat harvemmin täysin itsenäisesti toimivia yksiköitä, vaan niistä lähes poikkeuksetta on integraatioita muihin järjestelmiin, avoimiin tietolähteisiin, tunnistautumismekanismeihin, data-altaisiin sekä moniin muihin lähteisiin, joita järjestelmä käyttää hyväkseen.

Muun muassa näistä edellä mainituista syistä, On-Premise- konesalit ovat edelleen tarpeellisia ja ovat siinä mielessä yhä tärkeitä tietojärjestelmäarkkitehtuurissa ja niillä on oma tehtävänsä koko kokonaisuudessa. Sovelluksen käyttämän datan sijainnin vaatimus (EU tai Suomen valtionrajojen sisäpuolella) nousee esiin, mikäli järjestelmä pitäisi siirtää migraation avulla täysin pilveen tai jos se ylipäätään sijaitsisi alun perin pilvessä.

Mikäli sovellusdatan sijainnin vaatimus on Suomi, se on silloin organisaation oma tulkinta Vahti (Vahti, 2010) tai -Katakri (Katakri, 2015) ohjeeseen pohjautuen sekä se vaatii oman tietoturva ja riskinhallinnan linjauksen ja päätöksen asiasta organisaation sisällä.

Kumpikaan ohje ei suoraan kerro missä datan pitää sijaita. Suomessa on vain tullut yleinen konsensus organisaatioiden ja julkishallinnon sisällä siitä, että jos data-aineisto on luokiteltu niin, sen tulee sijaita suomessa.

Nämä yllämainitut seikat johtavat siihen, että käytännössä harva tietojärjestelmä voidaan toteuttaa puhtaasti pilvitoteutuksena ja niistä useimmin muodostuu hybridiympäristöjä. KEHA-keskuksen konesalipalvelut ovat siis toteutuksen osalta hybridiympäristöjä, jossa käytetään laaja-alaisesti hyväksi On-Premise ja pilvikonesaleja.

Muutokset ja vaikutukset, joita tehtiin On-Premise-ympäristöön pilvitoteutuksen yhteydessä, olivat teknisesti lähes minimaalisia. Pilvipalvelun testi -ja kehitysympäristötilit kytkettiin IPSEC VPN -yhteydellä VY-verkkoon. Tässä toteutusosassa käytettiin Microsoftin RRAS VPN -palvelin teknologiaa, joka on yhteystyypiltään dynaaminen VPN. Dynaaminen yhteystyyppi sallii joustavat yhdyskäytävät Azure-palveluihin, kuten rinnakkaiset Site to Point VPN-yhteydet. Staattista VPN-tyyppiä käytettäessä rinnakkaisen Site to Point VPN- palvelun käyttö ei ole mahdollista. Tätä yhteystyyppiä käytetään muun muassa konsulttien ja sovellustoimittajien tarvitsemissa yhteyksissä testi- ja kehitysympäristöjen virtuaalipalvelimiin tai muihin Azure-palveluihin, joita käytetään tietojärjestelmätoteutuksessa. Näiden yhteyksien avulla konsultit ja muut ulkopuoliset sovellustoimittajat pääsevät kehittämään palveluja turvallisesti IPSEC VPN -yhteyksien yli.

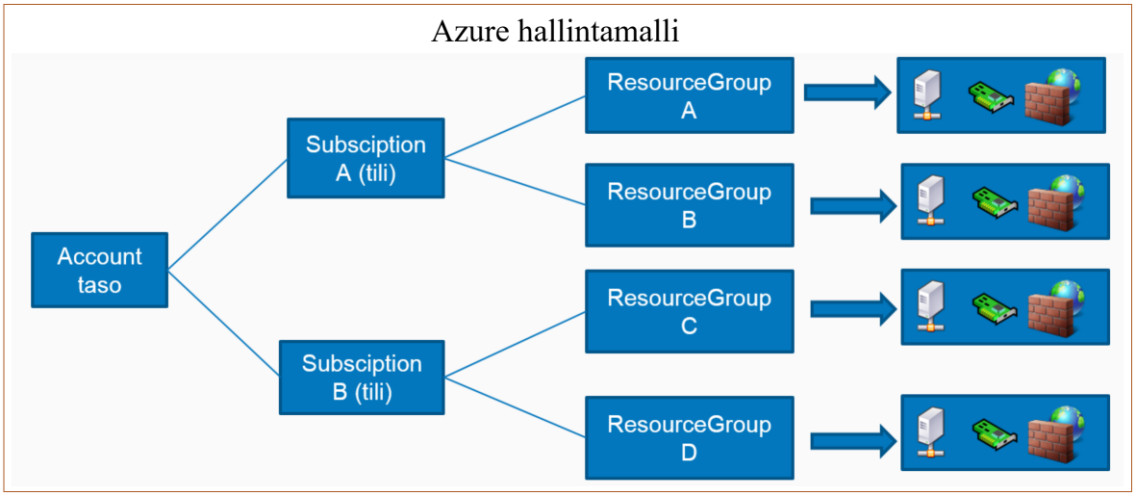
Tuotantoympäristö-tilin liitäntä VY-verkkoon (Subsription) toteutettiin hieman eri tavalla. Siinä käytössä on rautapohjainen VPN-laite, joka on kolmannen osapuolen valvonnassa ja hallinnassa 24/7. Tuotantoympäristöjen SLA-vaatimus on korkeammalla tasolla kuin testi- ja kehitysympäristöt, joten tällainen ratkaisu on perusteltu siltä osin.

Tietoisena valintana osana tietoturvaa oli staattisen VPN-yhteyden käyttäminen, joka käytännössä estää ulkopuolisten VPN-yhteyksien virittämisen tuotantoympäristöön. Tämä yhteys päätetään myös VY-verkkoon ja palvelut ovat sisäverkon asiakkaiden saavutettavissa VY-verkosta. Sisäverkon asiakkaat ovat lähinnä eri valtionhallinnon organisaatiot sekä ministeriöt.

Pääsynhallintaa tietoliikenteen tasolla VY-verkkoon rajataan perinteisellä palomuurilla. Tällä tavoin estetään tarpeeton liikenne tuotantoympäristöön sisäänpäin ja ulospäin suuntautuvan liikenteen osalta. Alla olevassa kuvassa havainnollistetaan, miten yhteydet on järjestetty KEHA Azure-pilven ja VY-verkon välillä.

6.2 KEHA-keskus pilvipalvelut toteutus

KEHA Azure toteutus toteutettiin hierarkiaperiaatteella, joka jäsentelee komponentit ja palvelut omiin siiloihinsa. Tällä tavoin saavutetaan hallinnoin näkökulmasta riittävä suoja ympäristöjen välillä.



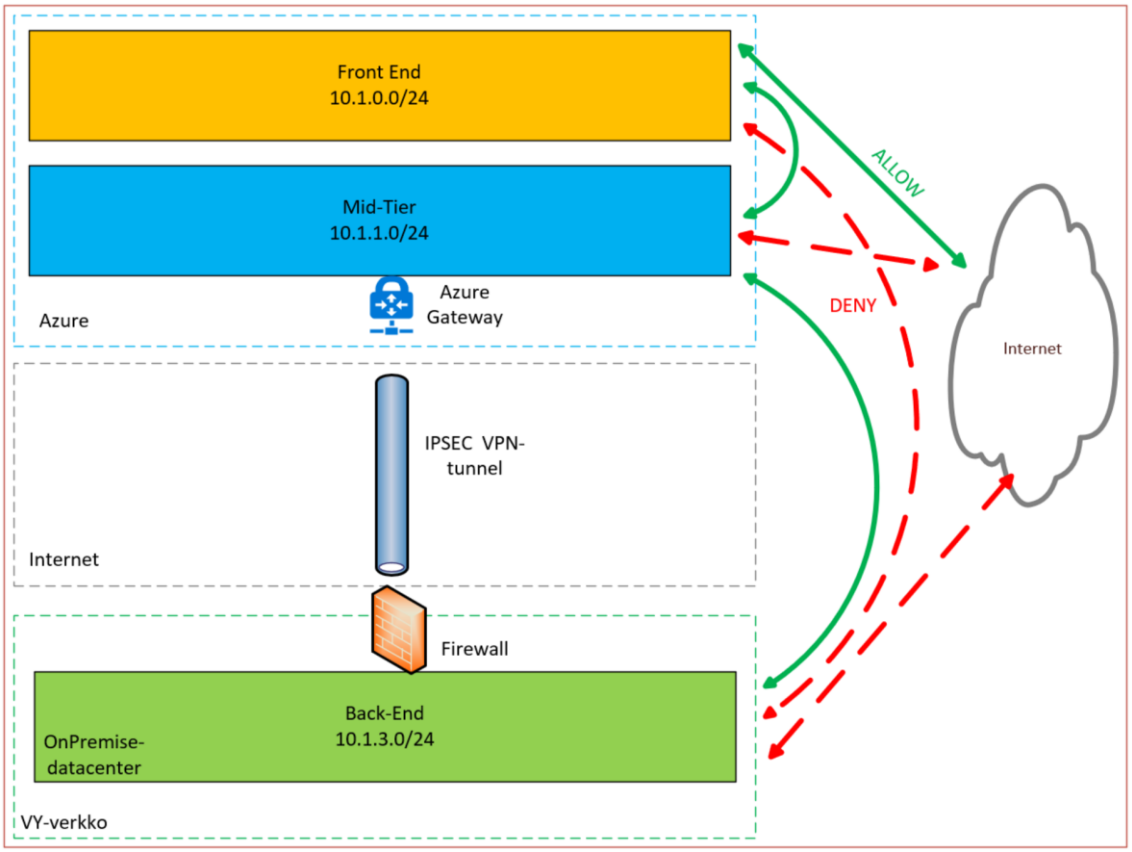
Kuva 12. KEHA-keskus Azure toteutuksen hierarkia hallinnan näkökulmasta.

Kuvassa 12. havainnollistetaan, miten palvelut rakennetaan järkevän hallintamallin mukaisesti. Azure Account-tasolla voidaan määritellä eri tilejä, joilla luodaan hallinnallisesta ja teknisestä näkökulmasta erottelua eri ympäristöjen välillä. KEHA-keskus päätyi ratkaisuun, jossa Azure-ympäristöön luotiin erilliset kehitys-, testi-, ja tuotantotilit. Tämä on tietoturvan kannalta tärkeä, koska tällä erottelulla kyseiset ympäristöt eivät kykene liikennöimään keskenään, mikäli sitä ei erikseen sallita.

Resurssiryhmillä (Resource Group) voidaan palvelukohtaisesti rajata yhden tilin sisällä komponentteja niin, että eri resurssiryhmät eivät liikennöi keskenään, mikäli sitä ei erikseen sallita. Tyypillisesti yksi tietojärjestelmäkokonaisuus sijoitetaan yhden ja saman resurssiryhmän sisään, jolloin siellä voi olla lukuisia eri Azure-komponentteja, joista palvelut rakentuvat. Kuten virtuaalipalvelin, verkkokortti, kiintolevy osio, palomuuri. Mikäli yksittäinen tietojärjestelmäpalvelu rakentuu useammasta eri virtuaalipalvelimesta tai muusta komponentista, niin ne sijoitetaan samaan resurssiryhmään.

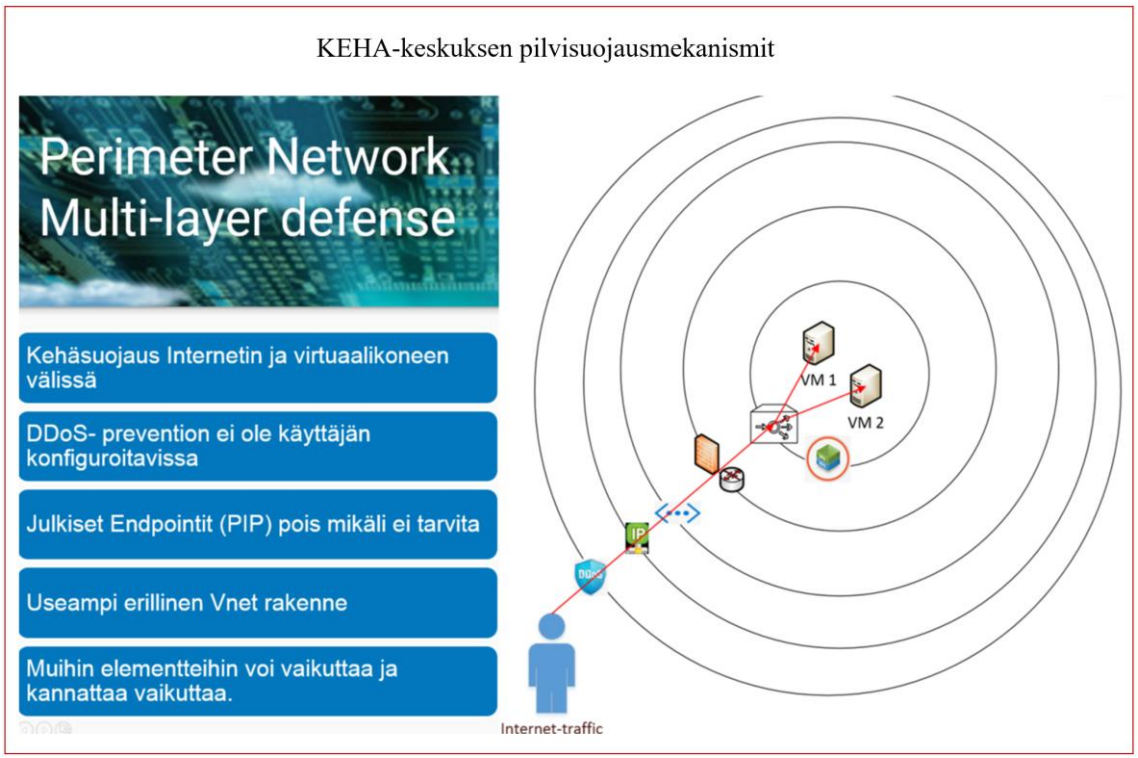
6.3 Tietoturva

KEHA-keskuksen Azure-ympäristön verkkotekninen toteutuksen fundamentaalinen osa on suunnitteluosiossa mainittu Azure Security Zone -model, turvavyöhykemalli.



Kuva 13. Sovellettu turvavyöhykemalli.

Tietojärjestelmien kannalta sekä tiedon sijainnin vaatimusten osalta verkkotekninen rakenne saattaa poiketa järjestelmäkohtaisesti hivenen alkuperäisestä suunnitelmasta siltä osin, että verkon suojatuin osa (Back-End) jossa sovelluksen käyttämä data saattaakin sijaita On-Premise-konesalissa (Kuva 13.). Tämän vuoksi toteutus tiettyjen järjestelmien osalta päädyttiin käyttämään soveltavasti suunnitteluosiossa mainitusta turvavyöhykemallia.



Kuva 14. KEHA-keskuksen pilvisuojausmekanismit.

Kuvassa 14. esitettävän uloimman kehän muodostaa DDoS-suojakerros, joka on Azuren fyysisen verkon kerroksessa. Se suojaa Azure-alustaa laajoilta internet-pohjaisilta hyökkäyksiltä. Tämän tyyppiset hyökkäykset käyttävät useimmiten BOT-verkon solmuja saadakseen mahdollisimman laajan hyökkäysarsenaalin eri lähteistä. Azuressa on pyritty rakentamaan vahva suojaverkko saapuvan ja lähtevän (Inbound/Outbound) liikenteen osalta. Suojaus toimii myös Azuren sisäisen liikenteen osalta, kuten esimerkiksi Pohjois-Amerikan ja Euroopan Azure alueen välisissä liittyntärajapinnoissa (Microsoft cloud services and network security, 2017).

Tämän suojakerroksen DDoS-palvelussa ei ole käyttäjän konfiguroitavia attribuutteja ja siihen ei ole minkäänlaista näkyvyyttä asiakkaan Azure-portaalista. Tämä on tavallaan Azure-tietoturvapalvelu, joka kuuluu palveluun automaattisesti ja siitä ei muodostu erillistä laskutusta asiakkaalle.

Käyttäjä voi luoda alemmissa kerroksissa suojamekanismeja pienemmän mittakaava DDoS-hyökkäyksiä vastaan, joten tämä ei pois-sulje ylemmän tason DDoS-valvontaa. Alemman tason suojamekanismeina voidaan käyttää Azure Marketplacen virtuaalisia palomuureja, jotka voidaan konfiguroida esimerkiksi valvomaan tietyn virtuaaliverkon (Vnet) liikennettä.

DDoS toiminnallisuus pystyy rajaamaan laajamittaiset hyökkäykset yhteen päätepisteeseen. Esimerkiksi ykksittäiseen virtuaaliseen palvelimeen, siihen kytkettyyn verkkokorttiin sekä siinä olevaan julkiseen IP-osoitteeseen. Mikäli käytössä on pienitehoinen virtuaalipalvelin, niin silloin Azuren DDoS-suojauskynnys ei välttämättä ylity ja siinä oleva IIS-palvelu saattaa kaatua ennen kuin DDoS-suojaus rekisteröi uhan.

6.4 Tulokset

Tässä kappaleessa on tarkoituksena avata tietoturvamekanismeja, joita KEHA-keskuksella on käytettävissä tietojärjestelmissä ja muussa IT-infrastruktuurissa. Käyttöönotetut tietoturva- ja suojausmekanismit tietojärjestelmäpalveluissa ja alustoissa mahdollistavat sen, että tietojärjestelmäympäristöjä voidaan perustellusti sijoittaa EUn alueella sijaitsevaan pilvipalveluun ja joka noudattaa EU alueen GDPR asetusta sekä EU mallisopimuslausekkeita tietoturvan ja tietosuojan osalta.

Esimerkiksi KEHA-keskuksen käyttämät Microsoft-konesalit Hollannissa (West Europe) ja Irlannissa (North Europe) täyttävät nämä vaatimukset niiltä osin. Osittain näitä mekanismeja voidaan toteuttaa myös On-Premise-konesaleissa. KEHA-keskus ei erottele tarkoituksenmukaisesti toisistaan pilvipalvelua ja On-Premise -konesaleja, vaan KEHA-keskus käsittelee niitä yhtenä kokonaisuutena tietojärjestelmän tuottamisen ja tietoturvamekanismien kannalta ns. hybridiratkaisuna.

KEHA-keskus käyttää pilvipalveluntarjoajina vain EU:n mallilausekkeita noudattavia toimittajia tietojenkäsittelijänä (kuten Microsoft). Tämä takaa KEHA-keskukselle ja sen

asiakkaille, että ne voivat hallita omia tietojaan ja että tietoja käsitellään tiukkojen tietosuojavaatimusten mukaisesti. KEHA-keskus ei käytä pilvipalveluntarjoajia, jotka eivät käytä EU:n mallilausekkeita. Nämä samat vaatimukset koskevat niin Suomesta tarjottavia paikallisia On-Premise- konesalipalveluja kuin pilvipalveluja.

EU:n mallilausekkeissa on tarkat tietosuojavaatimukset, joissa vaaditaan, että pilvipalveluntarjoajat käsittelevät asiakastietoja tiukan teknisen ja organisatorisen valvonnan mukaisesti. Toimittajan on noudatettava EU:n mallilausekkeissa määritetyt tietosuoja- ja tietoturvavaatimukset. Toimittajan tietosuojan valvonta ja prosessit tulee olla tasolla, jotka saavuttavat vähintään ISO 27001 -sertifioinnin edellyttämän taso. Toimittajan on osoitettava se, että saavutettu sertifiointi auditoidaan joka vuosi. Toimittajan on lisäksi toimittava avoimesti tietojen käsittelyssä ja heidän tulee ilmoittaa käsittelijöinä toimivat alihankkijat, tekniset ja organisatoriset turvatoimet, joilla suojataan asiakastietoja.

Tietoliikenteen salaus. Tietoliikenne salataan asiakkaan työaseman ja tietojärjestelmien välillä mm. https/ipsec protokollaa hyväksi käyttäen. Tietojärjestelmien välinen tietoliikenne salataan tapauskohtaisesti, mikäli palvelimet sijaitsevat toisiinsa nähden eri verkkoympäristöissä tai palvelun tiedonkäsittelylle asetetut vaatimukset vaativat salauksen saman verkkosegmentin sisällä.

Pilvipalvelun ja On-Premise-palvelinten välinen tietoliikenne kulkee salatun VPN-ratkaisun (IPSEC-tunneli) avulla päästä päähän niin, että liikenne kulkee suojattuna internetverkon ylitse. Palveluja suojataan aina On-Premise- ja pilvipalveluissa palomuureilla. Palomuureissa sallitaan rajatusti vain sellaiset protokollat, jonka avulla tietojärjestelmä kykenee toimimaan normaalilla ja sille ominaisella tavalla.

Tietoliikenne ja palveluverkot on segmentoitu turvavyöhykemallilla siten, että palvelulle muodostuu aina oma turvakerros. Edustaverkko (DMZ, Front-end), josta palvelut julkaistaan asiakkaille muodostaa puskurin asiakkaan ja tietojärjestelmät julkaisukerroksen välille. Seuraavassa kerroksessa on sovellusverkko (Mid-Tier) jossa palvelua ajetaan ja sitä voidaan kutsua verkkosegmentoinnin kannalta sovelluskerroksena. Kolmantena tausta-

verkko (Back-end) joka toimii tietokantakerroksena, johon tyypillisesti tehdään kattavimmat suojausmekanismit tietokantapalveluihin. Tämä on se verkkosegmentin osa joka suojatuin osa internetistä tai asiakasverkoista katsottuna. Asiakas-työasemilta ei missään tiedonkäsittelyvaiheessa muodostu suoria tietokantayhteyksiä, vaan välissä on aina sovellus- ja julkaisukerros. Internetistä on sallittu liikennöinti vain edustaverkkoihin, joka on loogisesti eriytetty muista alemmista verkkokerroksista. Liikennöinti on rajattu eri segmenttien välillä.

Monivaiheinen tunnistautuminen. Monivaiheista tunnistautumista käytetään pilvipalvelun hallintaan ja operointiin. Palveluun ei ole pääsyä pelkällä käyttäjätunnuksella ja salasanalla, vaan aina vaaditaan lisävahvistus, joka estää pilvipalvelujen operoinnin varastetulla tai muuten epävalidilla identiteetillä. Lisävahvistus voidaan tehdä joko soittamalla, tekstiviestillä tai mobiiliautentikointisovelluksella. Pilvipalvelun pääkäyttäjä- ja järjestelmätason oikeudet on rajattu hyvin pienelle joukolle.

Palvelinalustojen salaus. Salaus pyritään toteuttamaan mahdollisuuksien mukaan toteuttamaan jokaisella fyysisellä tai loogisella levyjärjestelmällä, sekä käyttöjärjestelmätasolla.

Tietokannan salaus. Tietokantapalvelu voidaan salata usealla eri tavalla, jolloin salausmekanismi muodostaa tietokantapalvelulle monta eri salauskerrosta. Itse tietokanta voidaan salata sekä kenttätason tietosisällön salaus, jolloin se muodostaa vähintään kolme eri salauskerrosta tietokantapalvelulle.

Tietosisällön anonymisointi. Henkilö- ja yritystiedot voidaan pseudonymisoida tai anonymisoida mikäli palvelun luonne niin vaatii. Niin pitkään, kun tietojen perusteella voi tunnistaa henkilön suoraan tai tiedot voidaan palauttaa takaisin tunnistettavaan muotoon, ne ovat yhä henkilötietoja ja niihin sovelletaan tietosuoja-asetusta. Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja. Tällaiset lisätiedot täytyy säilyttää huolellisesti erillään henkilötiedoista. Anonymisointi tarkoittaa henkilötietojen käsittelyä niin, että henkilöä ei

enää voida tunnistaa niistä. Anonymisoitua tietoa ei voi enää palauttaa alkuperäiseen muotoon, josta henkilöt ovat tunnistettavissa.

Salausavaimet ja varmenteet. Salausavaimia käytetään tietoliikenteen, palvelinten, tietokantojen sekä muiden komponenttien salaukseen. Salausavaimia käytettäessä STIV/STIII -tasolla tulisi täyttää Viestintäviraston kansalliset salausvaatimukset. Salausavainten vähimmäispituutena tulisi käyttää viestintäviraston ohjeistuksen ja suosituksen mukaisesti vähintään 3072 bitin avainpituutta. Salauksessa käytetään yleisesti turvalliseksi luokiteltuja salausprotokollia kuten SHA256 ja SHA512. Avaimen elinkaaren hallinta tulisi suhteuttaa avaimen mahdolliseen pituuteen. Mikäli ei ole mahdollisuutta käyttää 3072 bitin avainpituutta, niin avaimet tulisi uusia tihennetyin aikavälein. Mikäli pilvipalvelu- tai On-Premise-infrastruktuuri tukee maksimissaan 2048 bitin avainpituutta, niin salausavaimen uusimisen aikaväli toteutetaan tihennetysti.

Tiedon suojaaminen ulkopuolisilta. Jos pilvipalveluun tallennettaan salassa pidettävää tietoa, on varmistettava, että tietoon ei ole pääsyä muilla kuin hyväksytyillä sovituilla ja luotettavalla henkilöillä. Tiedon suojaamiseen ulkopuolisilta voidaan käyttää teknisiä keinoja, kuten salausta omalla avaimella. Lisäksi tiedon käsittelystä huolehtivien henkilöiden luotettavuus on selvitettävä joko itse, tai velvoitettava sopimuksessa palvelun tuottaja vastaamaan selvityksestä.

Kustannustehokkuus, joka oli työn yksi keskeisistä tavoitteista, toteutui toivotulla tavalla. Virtuaalipalvelinten käynnistys- ja pysäytysautomatiikka (Start/Stop automation) on laajamittaisessa käytössä, jossa virtuaalipalvelimet käynnistävät ja sammuvat käyttäjän määrittelemillä aikatauluilla. Tämä ratkaisu tarjoaa hajautetun edullisen automaatiovaihtoehdon käyttäjille, jotka haluavat optimoida virtuaalipalvelinten kustannuksia.

Edellä kuvatuilla periaatteilla KEHA-keskus voi minimoida tietoturvariskit pilvipohjaisissa, että muissa palvelumalleissa. Tietojärjestelmästä muodostuvat tiedonkäsittelyyn ja tiedon sijaintiin liittyvät riskit arvioidaan tapauskohtaisesti. On-Premise- palveluja käytetään vain, jos se on perusteltua tietoturva- tai tietosuojanäkökohdista.

7 JOHTOPÄÄTÖKSET

Työn keskeisinä tuloksina voidaan pitää sitä, että KEHA-keskuksella on nyt käytössä täysimittainen pilvipalveluinfrastruktuuri, johon on rakentunut testi- kehitys- ja tuotantoympäristöt, joissa voidaan kehittää, testata ja tuottaa tietojärjestelmäpalveluita. Tämä takaa sen, että jo tietojärjestelmän kehitysvaiheesta testaukseen ja siitä tuotantovaiheeseen saadaan tietojärjestelmälle identtinen alusta-arkkitehtuuri, jota ei tarvitse muuttaa.

Ympäristöissä hyödynnetään käynnistys- ja sammutusautomatiikkaa, joka tuo **kustannustehokkuutta**. Jokaisessa ympäristössä on identtinen verkkosegmentointiarkkitehtuuri, joka muiden tietoturvamekanismien avulla tuo ympäristöön kaivattua **tietoturvaa**. Tämän osalta toteutuu myös **ketteryys**, koska ympäristöt ovat rakennettu siten, että tietojärjestelmäprojektin alkuvaiheen infrastruktuurin rakentamiseen ei tarvitse keskittyä, vaan kaikki ovat valmiina projektin alkaessa.

Edellä kuvatuilla periaatteilla KEHA-keskus voi minimoida tietoturvariskit pilvipohjaisissa, että muissa palvelumalleissa. Tietojärjestelmästä muodostuvat tiedonkäsittelyyn ja tiedon sijaintiin liittyvät riskit arvioidaan tapauskohtaisesti. On-Premise- palveluja käytetään vain, jos se on perusteltua tietoturva- tai tietosuojanäkökohdista.

Toteuttamatta jäi Next Generation Firewall- eli keskitetty kaupallinen palomuuri pilviratkaisuna, jossa löytyy perinteisten palomuuritoiminnallisuuksien lisäksi sovellustason valvontaan liittyviä suojamekanismeja. Tämä ratkaisu tarjoaisi liki täydellisen näkyvyyden sovellusliikenteelle, ja joka muodostaisi erilaisia suojakerroksia palveluinfrastruktuuriin DDoS-hyökkäyksiä vastaan sekä kykenee suodattamaan haitallista bot-liikennettä ja kykenee toimimaan sovellushaavoittuvuuksia vastaan.

Tämä ratkaisu oli yhtenä vaihtoehtona harkinnassa, mutta se jäi toteuttamatta sen kustannusten ja hallinnoin kannalta. Tällaisen ratkaisun ylläpitämiseen tarvittaisiin korkeaa osaamista ja jatkuvaa ylläpitoa, sillä jokaisen järjestelmän tietoliikenne tulisi reitittää tämän ratkaisun kautta.

Merkitys julkishallinnon ja yleishyödyn kannalta on merkittävä, sillä pilviteknologian avulla organisaatiot ja julkishallinto kykenevät luomaan ja uudistamaan yhteisesti liiketoimintaa sekä toimintamalleja. Internet yhdessä pilviteknologian kanssa muodostavat yhden ison kokonaisuuden, jossa koko palveluketju on digitalisoitu.

Jatkotoimenpiteinä tulevaisuudessa on mm. ExpressRouten käyttöönotto pilvi-infrastruktuurissa, jossa nykyiset Site to Site -VPN ratkaisut korvataan tällä ratkaisulla. Se tuo lisää tietoliikennekapasiteettia ja tekee pilven käytöstä joustavampaa kuin mitä se nykyisellään on.

Lisäksi älykäs monivaihekirjautuminen (Multi factor authentication) asiakasidentiteettiin tullaan ottamaan käyttöön. Se tuo lisäturvaa käyttäjätunnuksen ja salasanan lisäksi, jossa käyttäjältä vaaditaan tietyissä tilanteissa lisävarmennusta. Tämä on hyvä keino ehkäistä luvattomia kirjautumisia pilvipalveluun, mikäli asiakkaan identiteetti olisi varastettu ja sitä käytettäisiin esimerkiksi ulkomailta käsin.

Tutkimuksen ja käytännön kokemusten perusteella PaaS-palveluita tulisi hyödyntää enemmän mitä pidemmälle organisaatio etenee pilvipalvelun käyttöönoton askeleissa. On luonnollista, että pilvipalvelua aloitteleva organisaation ensimmäiset käyttöönotettavat palvelut ovat juurikin IaaS-palveluita, koska se on turvallisempi lähestymistapa pilvipalvelun käytölle.

Tässä mallissa arkkitehtuuritapaa ei ikään kuin muuteta ollenkaan perinteisiin konesaleihin verrattuna, vaan samantyyppistä virtuaalipalvelinta ajetaan pilvipalvelussa kuin se olisi On-Premise-palvelussa. Tällaisessa tapauksessa palvelimen käyttökustannus ei juurikaan eroa perinteiseen malliin, vaan hyöty tulee käyttöönoton ketteryydestä ja palvelimen suorituskyvyn joustavuudesta.

PaaS-ratkaisusta tulee taas ilmiselvät hyödyt siitä, että itse palvelinta ei tarvitse ylläpitää. Joustavat automaatioskaalaukset kuormituksen mukaan ovat ilmiselvät hyödyt IaaS-ratkaisuihin verrattuna. On kuitenkin muistettava, että PaaS-palveluissa on myös rajoitteita,

jotka osaltaan hidastavat teknologian täysimittaista hyödyntämistä. Kuten erilaiset rajoitteet integraatiorajapintojen ja tietoliikenneverkkojen osalta. Teknologia kuitenkin myös tältä osin menee eteenpäin jatkuvasti ja nämä rajoitteet vähänevät yritysten vanhoihin järjestelmiin tulevaisuudessa. Tämä on sellainen osa-alue, joita pilvipalveluja harkitsevien organisaatioiden tulisi tutkia ensisijaisena palvelutuotannon muotona.

LÄHDELUETTELO

Aleem, A. & Sprott, C. R. 2013. Let me in the cloud: analysis of the benefit and risk assessment of cloud platform. Journal of Financial Crime. Saatavissa https://www-emeraldinsight-com.proxy.uwasa.fi/doi/pdfplus/10.1108/13590791311287337

Al, W. (2002). Server sandboxes: Dedicated hosting without the hassle. New Architect; 7, 11; ProQuest technology Collection.

Brian, O., Brunschwiler, T., Dill, H., Christ, H., Falsaf, B., Fischer, M., Grivas, S., Giovanoli, C., Gisi, R., Gutman, R. & others. (2012). Cloud Computing. White Paper SATW. Noudettu 15.1.2018 osoitteesta http://www.cloud-finder.ch/fileadmin/Dateien/PDF/News/2012-11-06_SATW_White_Paper_Cloud_Computing_EN_1_.pdf

Carroll, M., van der Merwe, A., Kotzé, P. (2011). Secure Cloud Computing Benefits, Risks and Controls. E-artikkeli. Paper presented at the 10th Annual Information Security for South Africa (ISSA) Conference, Johannesburg, South Africa. Saatavissa myös: http://ieeexplore.ieee.org/document/6027519/

Chen, Y., Sion, R. (2014). Costs and Security in Clouds. Network Security and Applied Cryptography Lab, Stony Brook University.

ENISA, European Network and Information Security Agency. Cloud Computing – Benif-tis, risks and recommendations for information security 2012. Noudettu 7.2.2018 osoit-teesta:https://resilience.enisa.europa.eu/cloud-security-and-resilience/publicati-ons/cloud-computing-benefits-risks-and-recommendations-for-information-security

Gibson, J., Eveleigh, D., Rondeau, R., Qing, T. (2012). Benefits and Challenges of Three Cloud Computing Service Models. Fourth International Conference on Computational Aspects of Social Networks (CASoN).

Gmach, D., Rolia, J., Cherkasova, L (2012). Comparing Efficiency and Costs of Cloud Computing Models. IEEE Network Operations and Management Symposium (NOMS): Short Papers

Goasduff, L. 2015. The financial case for moving to the cloud. Viitattu 13.11.2017. https://www.gartner.com/smarterwithgartner/the-financial-case-for-moving-to-the-cloud/

Heino, P. 2010. Pilvipalvelut (Cloud Computing). Helsinki: Talentum.

Hirsijärvi, S., Remes, P. & Sajavaara, P. (2009). Tutki ja kirjoita. Hämeenlinna: Kariston Kirjapaino Oy.

Järvinen, P., & Järvinen, A. (2011). Tutkimustyön metodeista. Tampere: Opinpajan kirja.

Longoria, G. 2016. TCO analysis demonstrates how moving to the cloud can save your Company money. Viitattu 20.04.2018. https://www.forbes.com/sites/moorinsights/2016/04/11/tco-analysis-demonstrates-how-moving-to-the-cloud-can-save-your-company-money/#57dc24897c4e

Microsoft, Start/Stop VMs during off-hours solution in azure automation. (2017). Noudettu 25.1.2018 osoitteesta https://docs.microsoft.com/en-us/azure/automation/automation-solution-vm-management

Microsoft, Cloud services and network security (2017). Noudettu 19.3.2018 osoitteesta: https://docs.microsoft.com/en-us/azure/best-practices-network-security

Mircea, M. & Andreescu, A. (2011). Using Cloud Computing in Higher Education: A Strategy to Improve Agility in the Current Financial Crisis. IBIMA Publishing Communications of the IBIMA,Vol. 2011, Article ID 875547, 15 pages. Noudettu 17.1.2018 osoitteesta http://ibimapublishing.com/articles/CIBIMA/2011/875547/875547.pdf

NIST (2011). The NIST Definition of cloud computing. Recommendations of the National Institute of Standards and Technology. Noudettu 19.7.2018 osoitteesta https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Pearl, N., Suganya, V. (2014). Secure Service to prevent Data Breaches in Cloud. International Conference on Computer Communication and Informatics.

Puolustusministeriö. Katakri (2015). Tietoturvallisuuden auditointityökalu viranomaisille. Noudettu 21.9.2018 osoitteesta https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

Radar, Tieto, VMware. The benefits of Cloud maturity, Cloud Maturity index 2017. Noudettu 19.1.2018 osoitteesta http://pages.tieto.com/Cloud-Maturity-Index-2017.html

Rajshri, P., Patel, V., Shrivastava, A. (2017). Cyber attack detection and classification using machine learning technique using Microsoft Azure cloud. Noudettu osoitteesta http://www.irjeas.org/wpcontent/uploads/admin/volume5/V5I2/IRJEAS04V5I204170617000009.pdf

Prashant, G. (2003). Power up N-more projects without waiting for new servers. ServerWorld; 17; 4; ProQuest

Tilastokeskus 2014. Tietotekniikan käyttö yrityksissä. Noudettu 20.12.2017 osoitteesta: http://www.stat.fi/til/icte/2014/icte_2014_2014-11-25_fi.pdf

Valtiovarainministeriö. Vahtiohje (2010). Tietojenkäsittelyn yleiset tietoturvavaatimukset. Noudettu 22.8.2018 osoitteesta: https://www.vahtiohje.fi/web/guest/tietojenkasittelyn-yleiset-tietoturvavaatimukset

Winkler, V. (2011). Securing the cloud: Cloud computer security techniques and tactics. Elsevier Science.

Woodside, A. (2010). Case study research: theory, methods and practice. England: Bradford Emerald Group Publishing 2010.