Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2019

Kari Vahteri

PILVIPALVELUT JA NIIDEN TIETOTURVA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikan insinööri

Huhtikuu 2019 | 43 sivua

Kari Vahteri

PILVIPALVELUT JA NIIDEN TIETOTURVA

Opinnäytetyön tavoitteena on parantaa ihmisten käsitystä pilvipalveluista ja niiden tietoturvasta. Pilvipalveluita on ollu yleisessä käytössä noin 10 vuotta. Pilvipalvelu käsitteenä tarkoittaa verkon yli tarjottavia palveluita.

Pilvipalvelut jaetaan kolmeen eri luokkaan SaaS- PaaS- ja IaaS-palveluihin, jotka tarkoittavat Ohjelmia palveluna, Alustaa palveluna ja Infrastruktuuri palveluna. Palvelumuotoja on myös erilaisia. Palvelumuodot määritellään Private Cloud, Hybrid Cloud tai Public Cloud palveluiksi. Private Cloud tarkoittaa että palvelut tulevat yrityksen omasta yksityisestä verkosta. Hybrid Cloud tarkoittaa että palvelut tulevat yrityksen yksityisestä verkosta sekä julkisesta internet-verkosta. Public Cloud tarkoittaa että palvelut tulevat pelkästään julkisesta internet-verkosta.

Yleisimpiä pilvipalveluiden tarjoajia ovat Microsoft Azure, Amazon Web Services ja Google Cloud Platform. Jokainen näistä tarjoaa laajan määrän erilaisia pilvipalveluita esimerkiksi tallennustilaa yrityksille ja yksityisasiakkaille.

Pilvipalveluiden tietoturva on ollut monien mietinnässä jo vuosien ajan, mutta jokainen pilvipalvelu tarjoaa kattavan määrän työkaluja ja ominaisuuksia, joilla asiakas voi suojata omat tietonsa yhtä turvallisiksi kuin ne olisivat yksityisessä verkossa.

ASIASANAT:

Pilvipalvelu, tietoturva, Microsoft Aure, Amazon Web Services, Google Cloud Platform.

BACHELOR´S | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of Engineering, Information and Communications Technology

April 2019 | 43 pages

Kari Vahteri

CLOUD COMPUTING AND THEIR SECURITY

The purpose of this thesis is to improve people's perception of cloud services and their security. There are about 10 years of cloud services in general use. Cloud service as a concept means services offered over the internet.

Cloud services are divided into three different categories of SaaS, PaaS and IaaS services, which mean Software as a service, Platform as a service and Infrastructure as a service. There are also different forms of service. Service forms are defined as Private Cloud, Hybrid Cloud, or Public Cloud services. Private Cloud means that services come from the company's own private network. Hybrid Cloud means that the services come from the company's private network and from the public Internet. Public Cloud means that services come exclusively from the public Internet.

The most common cloud providers are Microsoft Azure, Amazon Web Services and the Google Cloud Platform. Each of these offers a wide range of different cloud services, such as storage space for businesses and private customers.

The security of cloud services has been the subject of many people's reporting for years, but every cloud service provides a comprehensive set of tools and features that allow a customer to protect their own data as safe as they would in a private network.

KEYWORDS:

Cloud Computing, cloud security, Microsoft Azure, Amazon Web Services, Google Cloud Platform.

SISÄLTÖ

17

KUVAT

KÄYTETYT LYHENTEET

AWS	AWS (Amazon Web Services) Amazon Pilvipalvelu
EC2	EC2(Elastic Compute Cloud) Amazonin tarjoama pilvipalvelu.
GCP	GCP (Google Cloud Platform) Google Pilvipalvelu
IaaS	IaaS (Infrastructure as a service) Infrastruktuuri palveluna.
IoT	IoT (Internet of Things) Esineiden internet
NIST	NIST (National Institute of Standards and Technology)
PaaS	PaaS (Platform as a service) Kehtiysalusta palveluna.
SaaS	SaaS (Software as a Service) Ohjelmisto palveluna.

1 JOHDANTO

Opinnäytetyön aiheena on pilvipalvelut ja niiden tietoturva, sillä monet yritykset sekä yksityishenkilöt ovat siirtymässä pilvipalveluiden maailmaan. Pilvipalvelut ovat yleistyneet viimeisen kymmenen vuoden aikana, ja uskon, että ne tulevat yleistymään tulevaisuudessa vielä niin, että jokainen käyttää pilvipalveluita päivittäin. On siis tärkeää ymmärtää mistä pilvipalvelut ovat lähteneet ja ovatko ne niin turvallisia, että ne voivat olla osa yritysten ja yksityishenkilöiden jokapäiväistä elämää. Opinnäytetyössä käydään läpi pilvipalveluiden ominaisuuksia, jotta jokaisella sen lukeneella olisi parempi ymmärrys, mitä pilvipalveluilla voidaan tehdä. Lähdeaineisto koostuu suurimmaksi osaksi verkosta löytyvistä artikkeleista ja pilvipalvelun tarjoajien omista dokumentoinneista.

Opinnäytetyöni tarkoituksena on käydä ensin läpi pilvipalveluiden historiaa, että ymmärretään miten tähän tilanteeseen on päästy. Sen jälkeen käydään läpi pilvipalveluiden luokittelua, että ymmärretään minkälaisia pilvipalveluja on ja miten pilvipalvelut voidaan yhdistää yrityksen jo olemassa olevaan IT-infrastruktuuriin tai yksityishenkilön arjen tarpeisiin. Opinnäytetyössä käydään myös läpi tämän hetken suurimpia pilvipalvelun tarjoajia, sekä millaisia palveluita he tarjoavat. Lopuksi opinnäytetyö käsittelee näiden suurimpien pilvipalveluiden tietoturvaa, sekä millaisia työkaluja ja ominaisuuksia niissä on, joilla asiakas voi suojata omat tietonsa paremmin pilvipalveluissa.

2 PILVIPALVELU

NIST on vuonna 1901 perustettu Yhdysvaltojen kauppaministeriön liittovaltion virasto, jonka tarkoituksena on edistää Yhdysvaltojen innovaatioita ja teollisuuden kilpailukykyä edistämällä mittaustietoa, standardeja ja teknologiaa tavalla, joka parantaa taloudellista turvallisuutta ja parantaa elämänlaatua. NIST oli ensimmäinen standardeja luova organisaatio joka määritteli pilvipalvelut ja sen ominaisuudet, käyttöönoton ja palvelu mallit. (NIST 2008.) NIST:n mukaan Cloud computing (pilvipalvelu) on malli, joka luo mahdollisuuden kaikkialta kätevään tarvepohjaiseen verkkoliittymään. Pilvipalvelu jakaa tarpeen mukaan muokattavia tietokoneresursseja (kuten verkkoyhteyksiä, palvelimia, säilytystilaa, ohjelmia ja palveluita), jotka voidaan nopeasti kohdentaa ja saada käyttöön mahdollisimman pienellä palvelun tarjoajan työllä. Tämä pilvimalli koostuu viidestä tarpeellisesta ominaisuudesta, kolmesta palvelumallista ja neljästä käytäntöönpanomallista. (Mell & Grance 2011.)

Yleisesti pilvipalveluiksi lasketaan lähes kaikki verkon kautta toimivat palvelut. Pilvipalvelut ovat internetverkon kautta toimivia sovelluksia tai palveluita, joiden tarkoitus on helpottaa asiakkaan ohjelmien sekä palveluiden ylläpitoa. Pilvipalveluiden tarkoituksena on, että asiakas pääsee käsiksi erilaisiin ohjelmiin ja alustoihin pelkän verkkoselaimen avulla. Pilvipalvelut ovat myös halvempi tapa ylläpitää yrityksen palvelimia, kun yrityksen ei tarvitse välttämättä itse ostaa palvelinlaitteita, eikä heidän tarvitse palkata henkilöstöä ylläpitämään palvelimia. Esimerkiksi Googlen sähköposti ja Google drive-palvelut ovat pilvipalveluita, jotka ovat laajalti käytössä niin yritysmaailmassa kuin yksityisillä käyttäjillä.

2.1 Pilvipalveluiden historia

Pilvipalvelut alkoivat ensimmäisen kerran saamaan muotoaan vuonna 1969. Ajatuksen pilvipalveluista loi ARPANET (Advanced Reasearch Projects Agency Network), joka oli nykypäivän internetin edelläkävijä. (Access Alto 2017.)

Alun perin idean tarkoitus oli yhdistää tietokoneita suurien matkojen yli tiede- ja puolustusvoimien tarkoituksiin. Teknologia kehitettiin keskusyksiköiden avulla, jotka kehitettiin 1950-luvulla. (Access Alto 2017.)

1990-luvun puolivälissä internetin käyttö laajeni, pelkkien yritysten tietokoneiden lisäksi verkkoon liittyi huomattava määrä yksityishenkilöiden tietokoneita. Vuosituhannen loppu toi tullessaan Salesforce.com nimisen yhtiön, joka ensimmäisenä tarjosi yritysohjelmistoja internetin välityksellä. Nykyisin tämä toiminto tunnetaan nimellä SaaS (Software as a service). (Access Alto 2017.)

Pilvipalvelut on ensimmäisen kerran mainittu vuonna 1996 artikkelissa, jossa Google CEO Erich Schmidt toi termin yleiseen käyttöön. Schmidt julkaisi tietoa, mihin kaikkeen pilvipalveluja voitaisiin käyttää. Kesti kuitenkin kymmenisen vuotta, ennen kuin ’pilvestä’ alettiin puhua avoimemmin. (Access Alto 2017.)

Google ja Microsoft käyvät tiukkaa kilpailua pilvipalveluiden tuomisesta yleiseen käyttöön. Google julkaisi 2009 Google Appsin minkä avulla ihmiset voivat käyttää pilvipalveluja. Microsoft ei ole ollut kilpailussa paljoa jäljessä ja tiukka kilpailu yritysten välillä jatkuu yhä edelleen. Onneksi tämä yritysten välinen kilpailu on ajanut pilvipalveluja kovaa vauhtia eteenpäin. (Access Alto 2017.)

Vuoden 2009 lopulla pilvipalvelut valtasivat startup-yritys markkinat. Tämän johdosta ne levisivät nopeasti monien yritysten käyttöön. Amazon nousi nopeasti suureksi nimeksi haalimalla hyvin tunnettuja nimiä kuten Netflix ja Nasan Mars Curiosity Rover.

Pilvipalveluiden käytön laajenemisen myötä olemme nähneet dramaatisen kasvun niin Paas, Saas kuin IaaS palveluissa. Tämän lisäksi tietoturva yritykset ovat kasvaneet vuosien varrella vastaamaan pilvipalveluiden alati muuttuvasta tietoturvasta. (Access Alto 2017.)

Pilvipalvelujen synty on peräisin siis useista eri teknologioista, jotka myöhemmin loivat pilvipalvelut sellaiseen muotoon kuin me nykypäivänä ne tunnemme. Todennäköisesti tulevan kymmenen vuoden aikana pilvipalvelut tulevat olemaan osa jokaista yritystä. (Access Alto 2017.)

.

2.2 Pilvipalvelut käytännössä

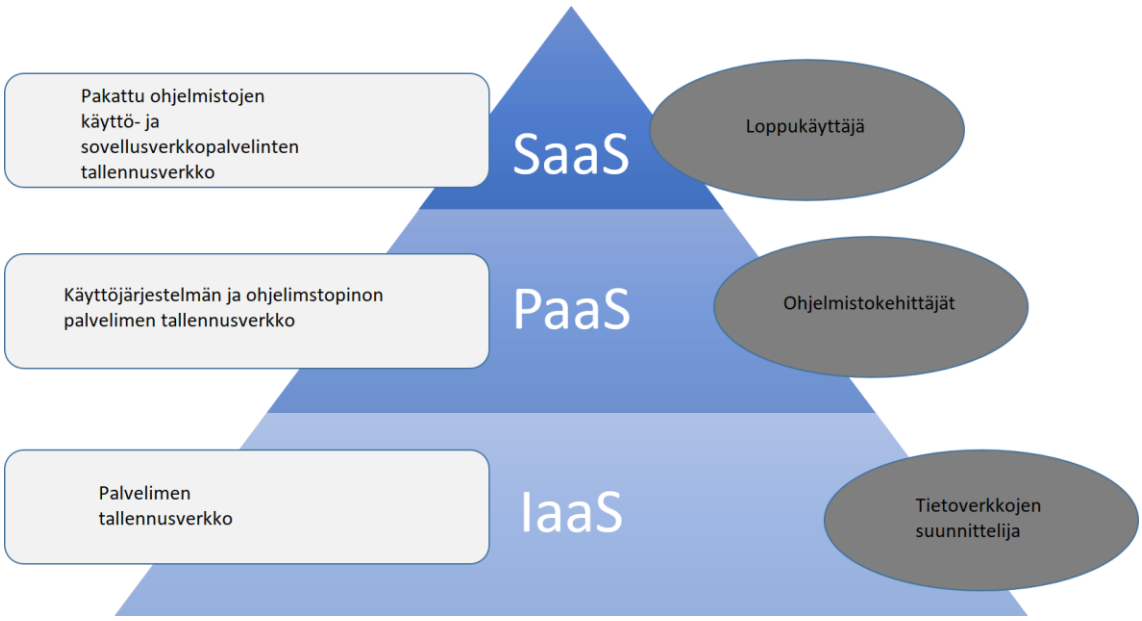
Pilvipalvelut ovat käytänössä erilaisia sovelluksia ja palveluita joilla yritykset ja yksityiset henkilöt pyrkivät helpottamaan jokapäiväisiä IT toimiaan.

Pilvipalvelujen avulla yritys pystyy pienentämään kustannuksiaan, koska tällöin ne eivät joudu investoimaan kalliisiin palvelimiin, eikä niiden tarvitse ylläpitää omia palvelimia. Kustannuksia pienentää myös se, että maksetaan vain tarvittavista IT-palveuista ilman huolta riittäisikö omien laitteiden kapasiteetti hoitamaan tarvittavat palvelut. Yksi hyvä esimerkki pilvipalvelusta on Microsoft office 365. Sen avulla yritys saa monia eri palveluita kuten sähköpostipalvelun, laskentataulukkosovelluksen sekä monia muita sovelluksia joita yritys tarvitsee.

Pilvipalvelut tarjoavat myös yksityishenkilöille hyödyllisiä palveluita. Esimerkiksi Google G Suite sisältää sähköpostipalvelun, mutta myös monia muita ominaisuuksia kuten esimerkiksi Google drive palvelun. Siihen käyttäjä voi tallentaa omia tiedostojaan ja vaikka halutessaan taulukkolaskentaohjelman millä seurata omia kulujaan.

3 PILVIPALVELUIDEN LUOKITTELU

Tämän kappaleen tarkoituksena on selventää mitä SaaS, PaaS ja IaaS palvelut ovat. Kuva 1 selventää näitä käsitteitä. Vasemmalta näkee, mitä palvelut voivat sisältää ja oikealla näkee kenelle ne voisivat olla suunnattu. Luvussa selvennetään lisäksi mitä Hybrid Cloud, Public Cloud, ja Private Cloud ovat, sekä millaisessa käytössä niistä voi hyötyä.



Kuva 1. SaaS, PaaS ja Iaas palveluiden rakenne (codematters 2017.)

3.1 PaaS (Plafrom as a Service)

PaaS- palvelumalli tarjoaa palveluja, jotka kohdistuvat erityisesti kehittäjille, jotka voivat käyttää jaettuja työkaluja, prosesseja sekä sovellusliittymiä nopeuttamaan sovellusten kehittämistä, testausta ja käyttöönottoa. Yrityksille PaaS voi varmistaa, että kehittäjillä on valmiudet käyttää resursseja, seurata tiettyjä prosesseja ja käyttää vain rajattuja palveluita, kun taas operaattorit ylläpitävät taustalla olevaa infrastruktuuria. (Knorr 2018).

PaaS tarjoaa täysin virtuaalisen palvelinympäristön, josta asiakas saa tietyn lohkon palveluita. PaaS-malli tarjoaa eniten asiakkaalle, joka haluaa itse rakentaa omat sovelluksensa. ”Tässä toteutustavassa asiakkaan käyttöliittymä on

ohjelmistokehitysväline ja jonkinlainen palvelussa oleva hallintakonsoli. Loppukäyttäjä pääsee sovellukseen toki selaimen välityksellä. PaaS-koneiston käyttäminen tuontantosovellusten ajamiseen ei onnistu lennossa. Asiakkaalta tarvitaan jonkin verran viitseliäisyyttä, jotta ympäristö saadaan pystyyn ja sinne syntyy tarpeelliset ylläpitorutiinit.” (Heino 2010.)

Yleisimpiä PaaS-palveluja ovat Amazon Web Services, SalesForce, Microsoft Azure ja Google App Engine.

3.2 IaaS (Infrastructure as a Service)

Perustasolla IaaS:n julkiset pilvipalveluntarjoajat tarjoavat tallennus- ja laskentapalveluja käyttömaksua vastaan. Kaikkien suurten julkisten pilvipalvelujen tarjoamat palvelut ovat kuitenkin hämmästyttäviä: erittäin skaalautuvat tietokannat, virtuaaliset yksityiset verkot, suuren datan analytiikat, kehitystyökalut, koneellinen oppiminen, sovellusten valvonta ja niin edelleen. Amazon Web Services oli ensimmäinen IaaS-palveluntarjoaja ja johtaa edelleen markkinoita. Niitä seuraa Microsoft Azure, Google Cloud Platfrom ja IBM cloud. (Eric Knorr 2018).

”Infrastructure as a Service- eli IaaS-typpisessä pilvipalvelussa tarjoaja ylläpitää internetissä virtuaalista konesalia tai konesaleja, lohkoo sieltä asiakkaille etukäteen määriteltyjä ja hinnoiteltuja osioita ja antaa ne asiakkaan käyttöön.” (Petteri Heino 2010) Tämä tarkoittaa sitä, että palvelun tarjoaja ylläpitää itse virtuaalisia koneita ja verkkoja omissa tiloissaan, joita tarjoaja sitten käytännössä vuokraa asiakkaille ja asiakkaat voivat näihin lohkoihin asentaa omat ohjelmansa. Palvelun tarjoaja luo vain omiin palvelimiinsa asiakkaan tarvitseman infrastruktuurin virtualisesti ja sen infrastruktuurin perusteella palvelun tarjoaja määrittelee hinnan.

Yleisimpiä IaaS-palvelun tarjoajia ovat esimerkiksi Amazon Web Services, Microsoft Azure ja Google Computer Engine.

3.3 SaaS (Software as a Service)

Tämän tyyppinen julkinen pilvipalvelu tarjoaa sovelluksia Internetselaimen kautta. Yrityksien suosituimmat SaaS-sovellukset löytyvät Googlen G Suite -palvelusta ja Microsoftin Office 365:stä. Lähes kaikki yrityssovellukset, mukaan lukien Oracle- ja SAP-

ERP-sviitit, ovat ottaneet käyttöön SaaS-mallin. Yleensä SaaS-sovellukset tarjoavat laajan kokoonpanovaihtoehdon sekä kehitysympäristöjä, joiden avulla asiakkaat voivat koodata omat muutokset sekä lisäykset. (Eric Knorr 2018)

”Software as a Service- eli SaaS-tyyppisessä pilvipalvelussa asiakas hankkii itselleen pelkän sovelluksen. Sovellus jaetaan tietoliikenneyhteyden avulla loppukäyttäjän selaimeen.” (Petteri Heino 2010).

SaaS palvelut tarjoavat siis käyttäjilleen ohjelmia selaimen avulla. SaaS palvelut helpottavat monen käyttäjän arkea, kun asiakkaan itse ei tarvitse huolehtia sovelluksien päivittämisestä eikä ylläpidosta, vaan palveluntarjoaja hoitaa päivittämisen ja ylläpidon asiakkaan puolesta.

Yleisimpiä SaaS palvelun tarjoajia ovat Amazon Web Services, Microsoft office 365 sekä Google G Suite.

3.4 Public Cloud

Julkinen pilvi määritellään kolmannen osapuolen palveluntarjoajien tarjoamiksi tietokonepalveluiksi julkisessa Internetissä. Tällöin ne ovat kaikkien saatavilla, jotka haluavat käyttää tai ostaa niitä. Ne voivat olla maksuttomia tai niitä voidaan myydä tilauksesta, jolloin asiakkaat voivat maksaa vain kulutusyksikköä kohti kuluttamansa CPU-syklin, tallennuksen tai kaistanleveyden. (Microsoft Azure What is Public Cloud).

Toisin kuin yksityistet pilvipalvelut, voi julkisen pilven käyttö tuoda yritykselle säästöjä kalliista kustannuksista, jotka aiheutuvat paikallisten laitteistojen ja sovellusinfrastruktuurien hankinnasta, hallinnasta ja ylläpidosta. Pilvipalvelujen tarjoaja on vastuussa järjestelmän hallinnasta ja ylläpidosta. Julkisia pilviä voidaan käyttää myös nopeammin kuin paikallisia infrastruktuureja ja erittäin skaalautuvaa alustaa. Jokainen yrityksen työntekijä voi käyttää samaa sovellusta mistä tahansa, toimistosta tai sivukonttorista, valitsemallaan laitteella niin kauan kuin voivat käyttää Internetiä. Turvallisuutta koskevat huolenaiheet on nostettu julkisiin pilviympäristöihin. Kun julkinen pilvipalvelu toteutetaan oikein, se voi olla yhtä turvallinen kuin tehokkain hallittu yksityinen pilvitoimintamalli. Tämä edellyttää, että palveluntarjoaja käyttää asianmukaisia turvamenetelmiä, kuten tunkeutumisen havaitsemis- ja estojärjestelmiä (IDPS). (Microsoft Azure What is Public Cloud).

Public Cloud eli julkinen pilvi on siis hyödyllinen tapa käyttää pilvipalveluja. Saman yrityksen eri henkilöt voivat käyttää samoja tiedostoja, vaikka he olisivat eripuolella maailmaa, kunhan heillä on yhteys internetiin.

3.5 Private Cloud

Yksityinen pilvi määritellään tietokonepalveluiksi, joita tarjotaan joko Internetin tai yksityisen sisäisen verkon kautta käyttäjien valitsemiseksi yleisön sijasta. Yksityisiä pilvipalveluja kutsutaan myös sisäiseksi tai yrityskohtaiseksi pilveksi. Se tarjoaa yrityksille monia julkisen pilven etuja, kuten itsepalvelun, skaalautuvuuden ja joustavuuden, lisävalvonnalla ja räätälöinnillä, joka on käytettävissä omistetuista resursseista paikan päällä sijaitsevan tietotekniikan infrastruktuurin yli. Lisäksi yksityiset pilvet tarjoavat korkeamman turvallisuustason ja yksityisyyden sekä palomuurien että sisäisen hosting-palvelun avulla. Tällä varmistetaan, että kolmannen osapuolen palveluntarjoajat eivät voi käyttää tietoja ja arkaluonteisia tietoja. Yksi haittapuoli on se, että yrityksen tietotekniikkaosasto vastaa yksityisen pilven hallinnasta aiheutuvista kustannuksista ja vastuullisuudesta. Joten yksityiset pilvet vaativat samat henkilöstö-, hallinto- ja ylläpitokustannukset kuin perinteisessä datakeskuksessa. (Microsoft Azure What is Private Cloud)

Pilvipalvelujen kaksi mallia voidaan toimittaa yksityisellä pilvellä. Ensimmäinen on infrastruktuuri palveluna (IaaS), jonka avulla yritys voi käyttää palveluina infrastruktuuriresursseja, kuten laskentaa, verkkoa ja tallennusta. Toinen on alusta palveluna (PaaS), jonka avulla yritys pystyy toimittamaan kaiken yksinkertaisista pilvipohjaisista sovelluksista hienostuneisiin yrityssovelluksiin. Yksityiset pilvet voidaan yhdistää myös julkisiin pilvipalveluihin hybridi-pilven luomiseksi. Tällöin yritys voi hyödyntää pilvipurkausta vapauttamaan enemmän tilaa ja mittakaavaa laskentapalveluja julkiseen pilviin, kun tietotekniikan kysyntä kasvaa. (Microsoft Azure What is Private Cloud)

Yksityinen pilvi eli Private Cloud on hyvä ratkaisu yrityksille joilla tietoturva on tarkkaa. Tämä kuitenkin edellyttää, että yrityksellä tulee olla riittävät resurssit toteuttamaan private cloud. Private cloud vaatii yritykseltä sen, että heillä on omat palvelimet sekä henkilöstöä joka hallitsee verkon luonnin ja ylläpidon, sekä palveluiden luonnin ja ylläpidon

3.6 Hybrid Cloud

Hybridipilvi on laskentaympäristö, joka yhdistää julkisen pilven ja yksityisen pilven sallimalla tietojen ja sovellusten jakamisen niiden kesken. Kun tietojenkäsittely- ja prosessointikysyntä vaihtelee, hybridilaskennan avulla yritykset voivat skaalata saumattomasti paikallisen infrastruktuurinsa julkiseen pilviin. Tällöin yritys voi käsitellä ylivuotoa, ilman että kolmannen osapuolen tietokeskukset pääsevät käyttämään kaikkia niiden tietoja. Organisaatiot saavat yleisen pilven joustavuuden ja laskentatehon perus- ja ei-herkille tietojenkäsittelytehtäville, mutta pitävät liiketoimintakriittiset sovellukset ja tiedot paikan päällä turvallisesti yrityksen palomuurin takana. (Microsoft Azure What is Hybrid Cloud)

Hybridi-pilven avulla yritykset eivät voi vain laskea tietojenkäsittelyresursseja, vaan se poistaa myös tarpeen tehdä massiivisia investointeja lyhyen aikavälin kysyntähuippujen käsittelemiseksi sekä silloin, kun yrityksen on vapautettava paikallisia resursseja herkempiin tietoihin tai sovelluksiin. Yritykset maksavat vain sellaisista resursseista, joita ne käyttävät tilapäisesti sen sijaan, että heidän tarvitsisi ostaa, ohjelmoida ja ylläpitää lisäresursseja ja laitteita, jotka voisivat jäädä käyttämättömiksi pitkiksi ajoiksi. Hybridilaskentatekniikka on "maailman paras mahdollinen" -ympäristö, joka tarjoaa kaikki pilvipalvelun edut - joustavuuden, skaalautuvuuden ja kustannustehokkuuden - mahdollisimman pienellä riskillä tietojen altistumiselle. (Microsoft Azure What is Hybrid Cloud).

Hybridi-pilvi on erinomainen vaihtoehto lähes jokaiselle yritykselle, jonka tarvitsee pitää joitain tietoja omilla palvelimillaan salassa, mutta tarvitsee myös public cloudin tuomia ominaisuuksia. Hybridi-pilvi vaatii kuitenkin, että yrityksellä on tarpeeksi resursseja pitää yllä omaa private cloudia sekä resursseja maksaa public cloudista tarpeen vaatiessa.

4 PILVIPALVELUIDEN EDUT JA RISKIT

Opinnäyttyön neljäs kappale käsittelee, mitä hyötyä ja mitä mahdollista haittaa pilvipaleluista voi olla yrityskäytössä sekä yksityiskäytössä.

4.1 Pilvipalveluiden edut

Pilvipalvelun avulla voi keskittyä enemmän yritykseen eikä datakeskusten hallintaan. Tietokeskusten hallinta ei ole useimpien yritysten keskeinen painopiste. Pilvipalvelun käyttäminen vapauttaa IT:n keskittymään sellaisten sovellusten kehittämiseen, joilla on liiketoiminta-arvo eikä datakeskuksen hallinta. Käyttämällä infrastruktuurin joustavia ominaisuuksia palveluna (IaaS) IT-infrastruktuuri voi kasvaa kysynnän kasvun tukemiseksi. Tällöin voidaan kehittää uusia sovelluksia nopeammin.

Käyttämällä alustaa palveluna (PaaS) yrityksesi pystyy kehittämään uuden tuotteen tai sovelluksen, tarjoamaan infrastruktuurin ja kehittämään uutta sovellusta paljon nopeammin kuin koskaan aikaisemmin. Pilvipalveluntarjoajan API:n hyödyntäminen voi auttaa automatisoimaan monia operatiivisia tehtäviäsi. Pilvipalveluntarjoajan tarjoamat sovellusohjelmointirajapinnat (API) ovat tärkeä osa siirtymistä DevOps-malliin. Sovellusliittymiä voidaan käyttää automatisointiin, seurantaan ja skaalaukseen. Pilvipalveluntarjoajan sovellusliittymän avulla voit käyttää useimpia, ellei kaikkia konsolin käytettävissä olevia toimintoja. API-menetelmät kehitetään ensin ja niitä käytetään portaalin tarvittavien toimintojen rakentamiseen.

Pilvipalvelut ovat skaalautuvia. Hyödyntämällä infrastruktuuria palveluna (IaaS) voit nopeasti rakentaa uuden infrastruktuurin uusien sovellusten tukemiseksi. Olettaen, että sovelluksesi on arkistoitu asianmukaisesti, koska sovelluksesi kuormitus kasvaa, voit skaalata vaakasuunnassa tarjoamalla uusia palvelimia. Jos sinun on lisättävä palvelimien kokoa tukemaan kuormituksia, jotka eivät pysty vaakasuoraan, voit järjestää suurempia palvelimia tukemaan lisääntyneitä vaatimuksia.

Pilvipalvelun taloudellinen merkitys on valtava. Infrastruktuurin vuokraus voi olla taloudellisesti järkevää. PAYG-malli on erityisen houkutteleva aloittelevien ja pienten yritysten rajalliselle kassavirralle. Pääomahankintoja ei tarvita ja laskentakustannukset voidaan laskea käyttökustannuksiksi. Kun infrastruktuuri ikääntyy, yritys ei joudu

hankkimaan uutta laitteistoa sen korvaamiseksi, vaan sille voidaan tarjota uusia palvelimia ikääntyvän laitteiston korvaamiseksi. Pilvipalvelun avulla yritys voi laajentaa maailmanlaajuista läsnäoloa. Cloud computingin avulla voidaan laajentaa maailmanlaajuista läsnäoloa nopeasti. SoftLayerissä on pilvipalvelukeskuksia ja läsnäolopisteitä (POP) eri puolilla maailmaa. Kukin näistä datakeskuksista on kytketty nopeiden kuitujen avulla, joten yritys voi koordinoida maailmanlaajuista infrastruktuuriaan. (Frank Bauerle 2014).

4.2 Pilvipalveluiden riskit

Huolimatta monista eduistaan pilvipalveluilla on myös haittoja. Yritysten, etenkin pienempien yritysten, on oltava tietoisia näistä haitoista ennen tämän teknologian käyttöönottoa. (Priya Viswanathan 2018)

Vaikka on totta, että tietoa ja tietoja pilvestä voidaan käyttää milloin tahansa ja mistä tahansa, joskus järjestelmällä voi olla vakavia toimintahäiriöitä. Käyttäjän tulee olla tietoinen siitä, että tämä tekniikka on aina altis katkoksille ja muille teknisille ogelmille. Jopa parhaille pilvipalveluntarjoajille voi tulla tällaisia ongelmia, huolimatta ylläpidon korkeista standardeista. Lisäksi tarvitaan erittäin hyvän Internet-yhteydet. Joskus saattaa tulla tilanteita, että verkko on ”jumissa” ja liitettävyyteen liittyen saattaa tulla ongelmia. (Priya Viswanathan 2018)

Toinen suuri ongelma pilvessä on turvallisuuskysymykset. Ennen tällaisen tekniikan käyttöönottoa, tulee ymmärtää, että yrityksen arkaluonteiset tiedot luovutetaan kolmannelle osapuolelle pilvipalvelujen tarjoajalle. Tämä saattaa saattaa yrityksen salassapidettävän tiedon vaaraan. Siksi tulee ehdottomasti varmistaa palveluntarjoajaa valittaessa, että valitsee luotettavimman palveluntarjoajan, jolla on osaamista pitää tiedot täysin turvassa. (Priya Viswanathan 2018)

Tietojen tallentaminen pilviin voi saattaa yrityksen alttiiksi ulkoisille hakkerointihyökkäyksille ja uhille. Internetissä mikään ei täysin turvallista ja siksi on aina otettava humioon, että siellä säilytettäviä tietoja voi joutua vääriin käsiin. (Priya Viswanathan 2018)

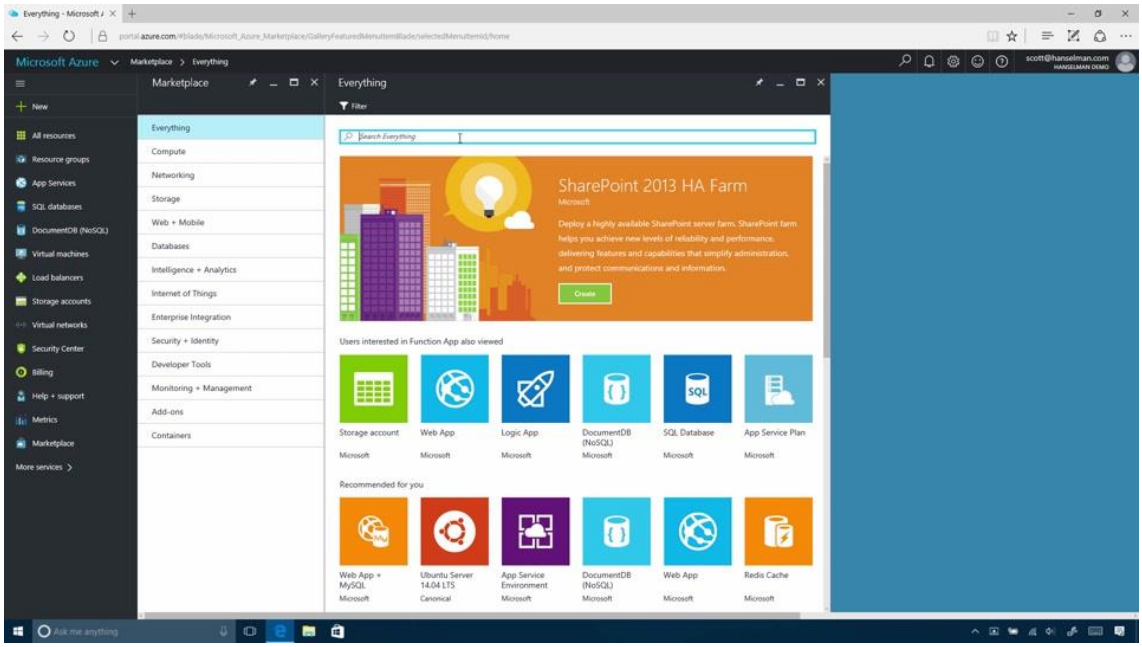
Kuten siis todettu pilvipalveluilla on hyvät ja huonot puolensa. Vaikka teknologia voi osoittautua suureksi hyödyksi sekä yrityskäytössä että yksityiskäytössä, voi se myös aiheuttaa haittaa, jos sitä ei ymmärrä ja käytetä oikein. (Priya Viswanathan 2018).

5 YLEISIMMÄT PILVIPALVELUT JA NIIDEN TARJOAJAT

Tämän kappaleessa käydään läpi yleisimmät pilvipalvelut ja niiden tarjoajat, miten kyseiset pilvipalvelut toimivat ja kenelle ne voivat olla suunnattu.

5.1 Microsoft Azure

Microsoft Azure tarjoaa käyttäjäystävällisen käyttöliittymän missä on paljon valmiita työkaluja. Kuva 2 havainnollistaa miltä Microsoft Azuren käyttöliittymä näyttää.



Kuva 2. Microsoft Azure käyttöliittymä. (Hanselman S. 2019).

Azure on julkinen pilvipalvelualusta, jossa on palveluja, kuten infrastruktuuri palveluna (IaaS), alusta palveluna (PaaS) ja ohjelmisto palveluna (SaaS), joita voidaan käyttää esimerkiksi analytiikan seuraamiseen, virtuaalisien palvelujen tietojenkäsittelyyn, datan tallentamiseen sekä moneen muuhun asiaan. Sitä voidaan käyttää korvaamaan tai täydentämään omia palvelimia. (Nicole Shortslef.)

Azure on julkinen pilvipalvelualusta, joka tukee laajaa valikoimaa käyttöjärjestelmiä, ohjelmointikieliä, kehyksiä, työkaluja, tietokantoja ja laitteita. Azure on nopea, joustava

ja edullinen alusta, jonka hinnoittelu ja ominaisuudet tekevät siitä yhden parhaista pilvipalveluista julkisen pilvipalvelun markkinoilla. (Nicole Shortslef.)

Azure on varmuuskopiointi- ja katastrofijärjestelmän unelma. Se on joustava, kehittyneen sivuston palauttamisen ja sisäänrakennetun integroinnin ansiosta. Azure-varmuuskopio tallentaa kolme kopiota tiedoista kolmeen eri paikkaan tietokeskuksessa, ja sitten vielä kolme kopiota kaukana olevaan Azure-tietokeskukseen, joten asiakkaan ei tarvitse koskaan huolehtia tietojen menettämisestä. (Nicole Shortslef.)

Jos asiakas käyttää myös Windows-irtuaaliympäristöä, Azuren sisäänrakennettu integrointi mahdollistaa lisävarmuuskopioien luonnin nopeasti. Azure-sivuston talteenotto integroituu System Center- ja HyperV-arkkitehtuureihin, mikä luo vahvan ja saumattoman yhteenkuuluvuuden Azuren, System Centerin ja HyperV:een välille. (Nicole Shortslef.)

Jos asiakan on etsimässä alustaa web-tai mobiilisovelluksen ylläpitoon, kehittämiseen tai hallintaan, Azure tekee näistä sovelluksista itsenäisiä ja mukautuvia korjaustiedostojen, automaattisen skaalauksen ja integroinnin avulla paikallisille sovelluksille. (Nicole Shortslef.)

Virtuaalikoneiden automaattisen korjauksen hallinnan avulla voidaan käyttää vähemmän aikaa infrastruktuurin hallintaan ja keskittyä sovellusten parantamiseen. Azure sisältää myös jatkuvan asennustuen, jonka avulla voidaan virtaviivaistaa käynnissä olevien koodien päivityksiä. (Nicole Shortslef.)

AutoScale on Azure Web Appsiin rakennettu ominaisuus, joka säätää resursseja automaattisesti asiakkaan web-liikenteen perusteella, jotta asiakkaalla on tarvittavat resurssit, kun liikenne on korkea, ja säästää rahaa, kun liikennettä on vain vähän. (Nicole Shortslef.)

Azuren kautta asiakas voi yhdistää verkkosovelluksensa saumattomasti sovellukseen. Sovellusten yhdistäminen molemmissa paikoissa antaa sekä työntekijöille että kumppaneille turvallisen pääsyn palomuurin sisältämiin resursseihin, joita muutoin olisi vaikea käyttää ulkoisesti. (Nicole Shortslef.)

Azure voi integroida asiakkaan Active Directoryn täydentämään identiteetti- ja käyttöominaisuuksia. Tämä antaa DNS:lle maailmanlaajuisen ulottuvuuden keskitetyn hallinan ja hyvän turvallisuuden. (Nicole Shortslef.)

Azure-sovelluksen avulla voi jakaa maailmanlaajuisesti Active Directory -ympäristön, jolla on suora yhteys asiakkaan omaan Active Directory palveluun.Monet muut pilvipalvelun tarjoajat eivät pysty laajentaman verkkotunnuksen ohjaimen ulottuvuutta ja vakiinnuttamaan Active Directoryn hallintaa, kuten Azure. (Nicole Shortslef.)

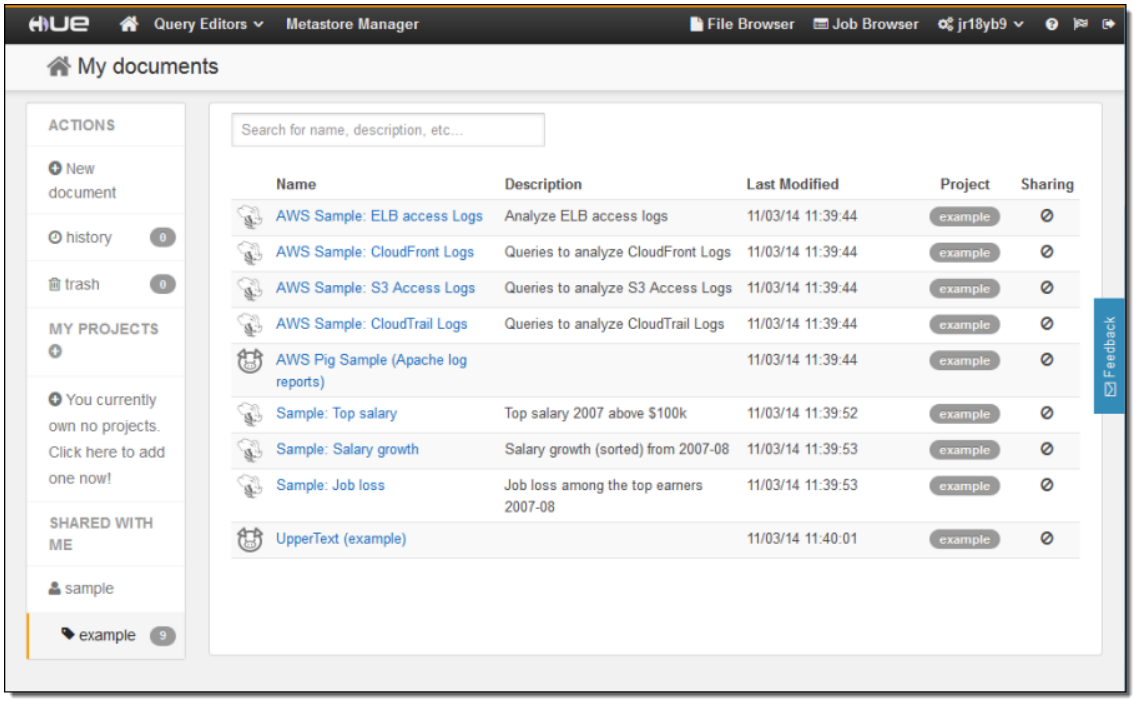
Jos asiakkaan käytössä on useita toimipaikkoja, asiakas käyttää sovelluksia tai pilvisovelluksia, kuten Office 365, Active Directoryn integrointi Azuren kanssa on keskeinen työkalu kaikkien näiden työkalujen hallintaan ja ylläpitoon. (Nicole Shortslef.)

Microsoft Azuren skaalautuvuus, joustavuus ja turvallisuus tekevät siitä täydellisen resurssin yrityksille, jotka liikkuvat IoT-ratkaisuihin (Internet of Things). Asiakas voi kytkeä laitteensa pilveen käyttämällä ratkaisuja, jotka integroituvat olemassa olevaan infrastruktuuriin ja aloittaa tietojen keräysprosessin asiakkaan yrityksestä. Azure IoT Hubissa asiakas voi seurata ja hallita miljardeja laitteita, joiden avulla asiakas voi tehdä parempia liiketoimintapäätöksiä, parantaa asiakkaiden kokemuksia, vähentää monimutkaisuutta, alentaa kustannuksia ja nopeuttaa kehitystä. Azuren turvallisuuden parantaminen on valtava voimavara IoT-ratkaisuille, joilla on perinteisesti turvallisuuseroja. Muita etuja ovat etävalvonta ja ennakoiva huolto ja analysointi. (Nicole Shortslef.)

Nämä neljä palvelua ovat vain vilkaisu siitä, mitä Azure voi tehdä asiakkaan ympäristön puolesta. Microsoftin määrittelemien palvelujen lisäksi se on täynnä pilvipalveluja, joita voidaan hyödyntää lähes millään tavalla asiakas itse haluaa. Jos asiakas on valmis kokeilemaan jotakin näistä palveluista, voi hän kokeilla näitä palveluja ilmaiseksi ja saada 200 dollaria Azure-krediittejä kokeilua varten. Asiakas voi myös saada käsityksen kustannuksista hinnoittelulaskimen avulla. (Nicole Shortslef.)

5.2 Amazon Web Services

Kuva 3 havainnollistaa Amazon Web Servicen käyttöliittymää, jonka avulla voi havaita, miten selkeäksi Amazon Web Servicen käyttöliittymä on tehty.



Kuva 3. Amazon web services käyttöliittymä. (Jeff Barr 2014).

Amazon Web Services (AWS) on kattava, kehittyvä pilvipalvelualusta, jonka Amazon tarjoaa. Se tarjoaa yhdistelmän infrastruktuuria palveluna (IaaS), alusta palveluna (PaaS) ja ohjelmistoja palveluna (SaaS).

AWS käynnisti vuonna 2006 Amazon.comin rakentaman sisäisen infrastruktuurin käsittelemään verkkokauppaa. AWS oli yksi ensimmäisistä yrityksistä, jotka ottivat käyttöön pay-as-you-go pilvipalvelu mallin. (Rouse M. 2017)

Amazon Web Services tarjoaa palveluja kymmeniltä tietokeskuksilta, jotka ovat levinneet saatavuusalueille eri puolilla maailmaa. Saatavuusalueet edustavat sijaintia, joka tyypillisesti sisältää useita fyysisiä datakeskuksia, kun taas alue on kokoelma saatavuusalueita maantieteellisellä läheisyydellä, jotka on yhdistetty matalan latenssin verkkoyhteyksiin. AWS-asiakas voi luoda virtuaalikoneita ja kopioida tietoja eri saatavuusalueen yksiköihin, jotta saavutetaan erittäin luotettava infrastruktuuri, joka kestää yksittäisten palvelimien tai koko datakeskuksen vikoja. (Rouse M. 2017)

Amazon Elastic Compute Cloud (EC2) tarjoaa virtuaalipalvelimia nimeltään instansseja laskentakapasiteetille. EC2-palvelu tarjoaa kymmeniä esimerkkityyppejä, joiden kapasiteetti ja koot vaihtelevat ja jotka on räätälöity tiettyihin työtyyppeihin ja sovelluksiin, kuten muistia vaativiin ja nopeutettuihin tietoihin. AWS tarjoaa myös automaattisen

skaalaustyökalun, jolla voidaan dynaamisesti skaalata kapasiteettia ylläpitämään suorituskykyä.

Amazon EC2 Container Service ja EC2 Container Registry mahdollistavat asiakkaiden mahdollisuuden työskennellä Dockerin konttien ja kuvien kanssa AWS-alustalla. Kehittäjä voi myös käyttää AWS Lambdaa palvelittomiin toimintoihin, jotka suorittavat automaattisesti sovellusten ja palveluiden koodin sekä AWS Elastic Beanstalk for PaaS. AWS sisältää myös Amazon Lightsailin, joka tarjoaa virtuaalisia yksityisiä palvelimia ja AWS-erän, joka käsittelee useita työvaiheita. (Rouse M. 2017)

Amazon Simple Storage Service (S3) tarjoaa skaalautuvan objektivaraston tietojen varmuuskopiointiin, arkistointiin ja analytiikkaan. Asiakas tallentaa tiedot ja tiedostot S3-objekteina, jotka voivat olla kooltaan jopa 5 Gt:n sisällä S3-bucketien sisällä, jotta ne pysyvät järjestyksessä. Yrityksellä on mahdollisuus säästää rahaa S3:lla sen tallennustilojen kautta tai käyttää Amazon Glacieriä pitkäaikaiseen varastointiin. (Rouse M. 2017)

Amazon Elastic Block Store tarjoaa lohkotason tallennustilaa pysyville tietojen tallennuksille käytettäväksi EC2-tapauksissa, kun taas Amazon Elastic File System tarjoaa hallittua pilvipohjaista tiedostojen tallennusta. (Rouse M. 2017)

Yritys voi myös siirtää tietoja pilviin tallennusliikennelaitteiden, kuten AWS Snowballin ja Snowmobilen, avulla tai käyttää AWS Storage Gateway -ohjelmaa, jotta paikalliset sovellukset pääsevät pilvipalveluihin. (Rouse M. 2017)

AWS tarjoaa hallittuja tietokantapalveluja Amazon Relational Database -palvelun kautta. AWS tarjoaa hallittuja NoSQL-tietokantoja Amazon DynamoDB: n kautta. (Rouse M. 2017)

AWS-asiakas voi käyttää Amazon ElastiCache- ja DynamoDB-kiihdytintä muistin välimuistina reaaliaikaisissa sovelluksissa. Amazon Redshift tarjoaa tietovaraston, joka helpottaa tietojen analysoijien suorittamaa liiketoimintatietojen suorittamista. (Rouse M. 2017)

AWS sisältää erilaisia työkaluja ja palveluja, joiden avulla käyttäjät voivat siirtää sovelluksia, tietokantoja, palvelimia ja tietoja julkiseen pilviin. AWS Migration Hub tarjoaa sijainnin, jolla voit seurata ja hallita siirtymiä tiloista pilviin. Pilvessä EC2 Systems Manager auttaa IT-tiimiä määrittämään paikalliset palvelimet ja AWS-tapaukset. (Rouse M. 2017)

Amazonilla on myös kumppanuuksia useiden teknologiatoimittajien kanssa, jotka helpottavat hybridilevyjen käyttöönottoa. VMware Cloud AWS:ssä tuo ohjelmistopohjaisen tietokeskusteknologian VMwaresta AWS-pilviin. Red Hat Enterprise Linux Amazon EC2: lle on toisen kumppanuuden tuote, joka laajentaa Red Hatin käyttöjärjestelmää AWS-pilviin. (Rouse M. 2017)

Amazon Virtual Private Cloud (VPC) antaa järjestelmänvalvojalle virtuaalisen verkon hallinnan AWS-pilven erillisen osan käyttämiseksi. AWS varaa automaattisesti uusia resursseja VPC:lle lisäsuojaa varten. (Rouse M. 2017)

Järjestelmänvalvojat voivat tasapainottaa verkkoliikennettä AWS-kuormituksen tasapainotustyökaluilla, mukaan lukien sovelluskuormituksen tasapainottaminen ja verkon kuormituksen tasapainottaminen. AWS tarjoaa myös verkkotunnusjärjestelmän nimeltä Amazon Route 53, joka ohjaa loppukäyttäjät sovelluksiin. (Rouse M. 2017)

Tietotekniikan ammattilainen voi luoda oman yhteyden paikalliseen tietokeskukseen AWS-pilviin AWS Direct Connect -palvelun kautta. (Rouse M. 2017)

Kehittäjä voi hyödyntää AWS-komentorivin työkaluja ja ohjelmistokehityspaketteja (SDK) sovellusten ja palvelujen käyttöönottoon ja hallintaan. AWS-komentoriviliitäntä on Amazonin omien koodien käyttöliittymä. Kehittäjä voi myös käyttää AWS-työkaluja Powershelliin hallitsemaan pilvipalveluita Windows-ympäristöistä ja AWS-palvelimettomasta sovellusmallista, jolla simuloidaan AWS-ympäristöä Lambda-toimintojen testaamiseksi. AWS SDK:t ovat saatavilla useille eri alustoille ja ohjelmointikielille, kuten Java, PHP, Python, Node.js, Ruby, C ++, Android ja iOS. (Rouse M. 2017)

Amazon API Gatewayn avulla kehitystiimi voi luoda, hallita ja seurata mukautettuja sovellusliittymiä, joiden avulla sovellukset voivat käyttää tietoja tai toimintoja back-end-palveluista. API-yhdyskäytävä hallitsee tuhansia samanaikaisia API-puheluita kerralla.

AWS tarjoaa myös pakattua media-transkoodauspalvelua, Amazon Elastic Transcoder palvelua, joka visualisoi mikropalvelupohjaisten sovellusten, AWS Step -toimintojen, työnkulun. (Rouse M. 2017)

Kehitystiimi voi myös luoda jatkuvaa integrointia ja jatkuvaa toimitusputkea palveluihin, kuten AWS CodePipeline, AWS CodeBuild, AWS CodeDeploy ja AWS CodeStar. Kehittäjä voi myös tallentaa koodin Git-arkistoihin AWS CodeCommitilla ja arvioida

mikropalvelupohjaisten sovellusten suorituskykyä AWS X-Ray -toiminnolla. (Rouse M. 2017)

Järjestelmänvalvoja voi hallita ja seurata pilvivarojen konfigurointia AWS Config- ja AWS Config -sääntöjen avulla. Nämä työkalut yhdessä AWS Trusted Advisorin kanssa voivat auttaa IT-tiimiä välttämään väärin määritettyjä ja tarpeettoman kalliita pilvivarojen käyttöönottoja. (Rouse M. 2017)

AWS tarjoaa portfoliossaan useita automaatiotyökaluja. Järjestelmänvalvoja voi automatisoida infrastruktuurin tarjoamisen AWS CloudFormation -mallien avulla sekä käyttää AWS OpsWorksia ja Chefia automatisoimaan infrastruktuurin ja järjestelmän kokoonpanot. (Rouse M. 2017)

AWS-asiakas voi seurata resurssien ja sovellusten tilaa Amazon CloudWatchin ja AWS Personal Health Dashboardin avulla sekä käyttää AWS CloudTrail -ohjelmaa säilyttääkseen käyttäjän aktiivisuuden ja sovellusohjelmointirajapinnan (API) auditointiin. (Rouse M. 2017)

AWS tarjoaa valikoiman pilvipalvelun palveluja, kuten AWS Identity- ja Access Management (IAM), jonka avulla järjestelmänvalvojat voivat määrittää ja hallita käyttäjien pääsyä resursseihin. Järjestelmänvalvoja voi myös luoda käyttäjän hakemiston Amazon Cloud Directoryn avulla tai liittää pilvivaroja olemassa olevaan Microsoft Active Directoryan AWS-hakemistopalvelun kanssa. Lisäksi AWS-organisaatiot voivat luoda ja hallita useita AWS-tilejä koskevia sääntöjä. (Rouse M. 2017)

Pilvipalvelujen tarjoaja on myös ottanut käyttöön työkaluja, jotka automaattisesti arvioivat mahdollisia turvallisuusriskejä. Amazon Inspector analysoi AWS-ympäristön sellaisiin haavoittuvuuksiin, jotka saattavat vaikuttaa turvallisuuteen ja vaatimustenmukaisuuteen. Amazon Macie käyttää konekieliteknologiaa arkaluonteisten pilvitietojen suojaamiseen. (Rouse M. 2017)

AWS sisältää myös työkaluja ja palveluja, jotka tarjoavat ohjelmisto- ja laitteistopohjaista salausta, suojaavat DDoS-hyökkäyksiä vastaan, tarjoavat Secure Sockets Layer- ja Transport Layer Security -sertifikaatteja ja suodattavat mahdollisesti haitallista liikennettä verkkosovelluksiin. (Rouse M. 2017)

AWS sisältää useita suuria datan analysointi- ja sovelluspalveluja. Amazon Elastic MapReduce tarjoaa Hadoop-kehyksen käsitellä suuria tietomääriä, kun taas Amazon

Kinesis tarjoaa useita työkaluja suoratoistodatan käsittelyyn ja analysointiin. (Rouse M. 2017)

AWS Glue on palvelu, joka käsittelee muutto-, muunnos- ja lataustöitä, kun taas Amazon Elasticsearch Service mahdollistaa tiimin suorittaa sovellusten seurantaa, lokianalyysia ja muita tehtäviä avoimen lähdekoodin Elasticsearch-työkalulla. (Rouse M. 2017)

Tietojen kyselyyn analyytikko voi käyttää Amazon Athenea S3:lle ja visualisoida sitten tiedot Amazon QuickSightilla. (Rouse M. 2017)

AWS tarjoaa laajan valikoiman AI-mallin kehittämis- ja toimitusalustoja sekä pakattuja AI-pohjaisia sovelluksia. Amazon AI -työkalujen sarja sisältää Amazon Lexin äänen ja tekstin chatbot-tekniikkaan, Amazon Polly tekstin puheeksi kääntämiseen ja Amazon Rekognition kuvien ja kasvojen analysointiin. AWS tarjoaa myös kehittäjille teknologiaa sellaisten älykkäiden sovellusten rakentamiseen, jotka perustuvat koneen oppimistekniikkaan ja monimutkaisiin algoritmeihin. (Rouse M. 2017)

AWS Deep Learning AMI:n avulla kehittäjät voivat luoda ja kouluttaa mukautettuja AI-malleja GPU: iden tai laskennallisesti optimoitujen instanssien klustereilla. AWS sisältää myös syvällisen oppimisen kehityskehykset MXNetille ja TensorFlowille. (Rouse M. 2017)

Kuluttajan puolella AWS-teknologiat käyttävät Alexa Voice -palveluita, ja kehittäjä voi käyttää Alexa Skills Kitia äänipohjaisten sovellusten rakentamiseen Echo-laitteille. (Rouse M. 2017)

AWS Mobile Hub tarjoaa joukon työkaluja ja palveluja mobiilisovellusten kehittäjille, mukaan lukien AWS Mobile SDK, joka tarjoaa koodinäytteitä ja kirjastoja. (Rouse M. 2017)

Mobiilisovelluksen kehittäjä voi myös käyttää Amazon Cognitoa hallitsemaan käyttäjien pääsyä mobiilisovelluksiin sekä Amazon Pinpointia lähettämään push-ilmoituksia sovellusten loppukäyttäjille ja analysoimaan näiden viestien tehokkuutta. (Rouse M. 2017)

AWS-viestipalvelut tarjoavat ydinviestinnän käyttäjille ja sovelluksille. Amazon Simple Queue Service on hallittu viestijono, joka lähettää, tallentaa ja vastaanottaa viestejä hajautettujen sovellusten komponenttien välillä varmistaakseen, että sovelluksen osat toimivat suunnitellusti. (Rouse M. 2017)

Amazon Simple Notification Service (SNS) antaa yritykselle mahdollisuuden lähettää pub-sub-viestejä päätepisteisiin, kuten loppukäyttäjiin tai palveluihin. SNS sisältää mobiiliviestitoiminnon, joka mahdollistaa push-viestien siirtämisen mobiililaitteisiin. Amazon Simple Email Service tarjoaa alustan IT-ammattilaisille ja markkinoijille lähettää ja vastaanottaa sähköposteja. (Rouse M. 2017)

Amazon Web Services -palvelussa on useita liiketoiminnan tuottavuuden SaaS-vaihtoehtoja. Amazon Chime -palvelu mahdollistaa online-videoneuvottelujen, puhelujen ja tekstipohjaisten keskustelujen käytön eri laitteissa. Yritys voi myös hyödyntää Amazon WorkDocsia, tiedostojen tallennus- ja jakamispalvelua sekä Amazon WorkMailia, joka on yritystoimintapalvelun kalenteritoimintoja. (Rouse M. 2017)

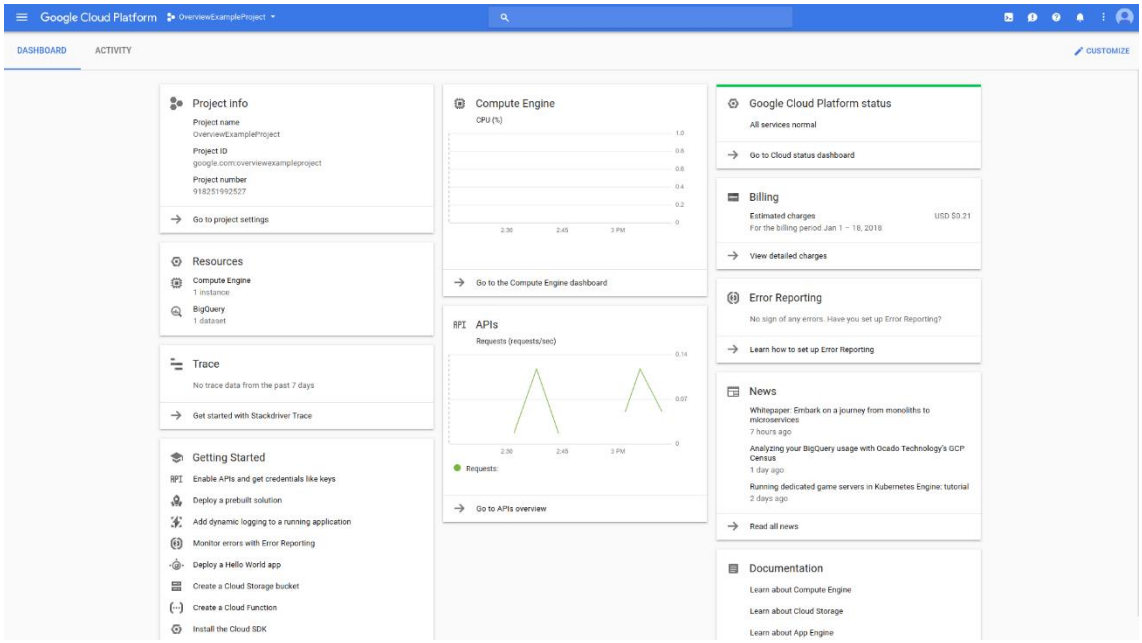
Työpöytä- ja streaming-sovelluspalveluihin kuuluvat Amazon WorkSpaces, etätyöpöytä-palvelin -ympäristö ja Amazon AppStream, palvelu, jonka avulla kehittäjä voi käyttää työpöytäsovellusta AWS: ltä loppukäyttäjän web-selaimelle. (Rouse M. 2017)

AWS: ssä on myös erilaisia palveluja, jotka mahdollistavat asiat internetin (IoT) käyttöönoton. AWS IoT -palvelun avulla voidaan hallita IoT-laitteita ja tietojen syöttämistä muihin AWS-tallennus- ja tietokantapalveluihin. AWS IoT -painike tarjoaa laitteistoa rajoitetulle IoT-toiminnolle, ja AWS Greengrass tuo AWS-laskentamahdollisuudet IoT-laitteisiin. (Rouse M. 2017)

AWS tarjoaa pilvipalveluihinsa pay-as-you-go -mallin joko tunnissa tai sekunnissa. On myös mahdollisuus varata tietty määrä laskentakapasiteettia alennettuun hintaan asiakkaille, jotka maksavat kokonaisuudessaan ennakkomaksun tai jotka kirjaavat yhden tai kolmen vuoden käyttösitoumukset. (Rouse M. 2017)

5.3 Google Cloud Platform

Kuva 4 havainnollistaa Google Cloud Platformin käyttöliittymää, joka tarjoaa selkeän näkymän, mitä pilvipalvelussa tapahtuu.



Kuva 4. Google Cloud Platform käyttöliittymä. (Google Cloud 2018).

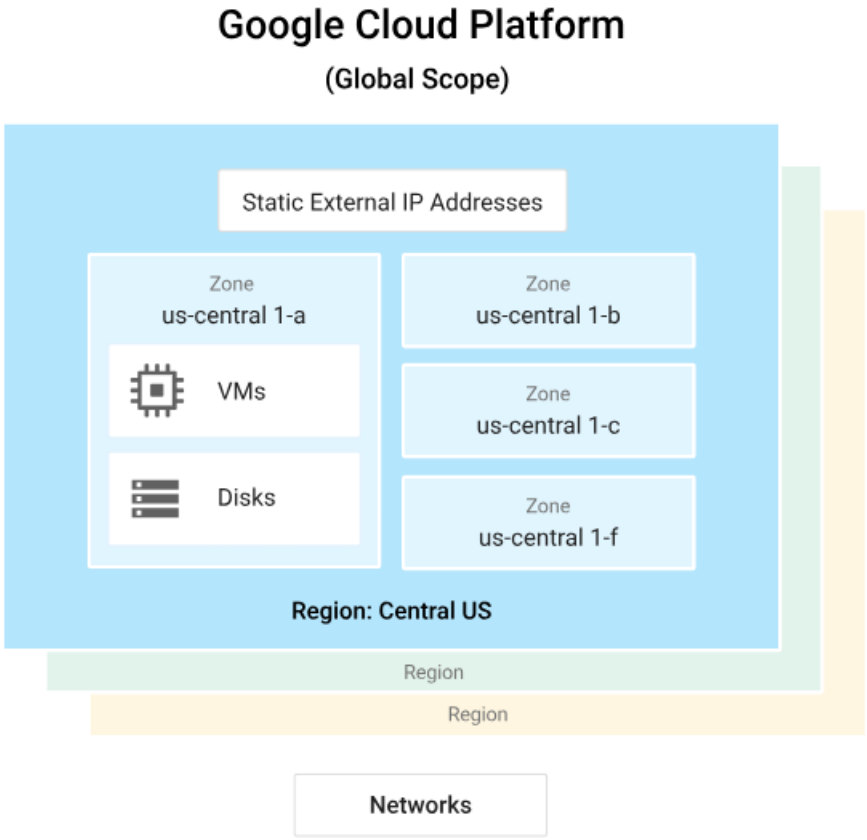
GCP koostuu joukosta fyysisiä omaisuuksia, kuten tietokoneita ja kiintolevyasemia, ja virtuaalisia resursseja, kuten virtuaalikoneita, jotka sisältyvät Googlen tietokeskuksiin ympäri maailmaa. Jokainen tietokeskuksen sijainti on globaalilla alueella. Alueita ovat Keski-USA, Länsi-Eurooppa ja Itä-Aasia. Jokainen alue on kokoelma vyöhykkeitä, jotka ovat erillään toisistaan alueella. Jokainen vyöhyke tunnistetaan nimellä, joka yhdistää kirjaintunnisteen alueen nimen kanssa. Esimerkiksi Itä-Aasian alueen vyöhyke a on nimeltään asia-east1-a. (Google Cloud Platform.)

Tämä resurssien jakelu tarjoaa useita etuja, mukaan lukien redundanssi vian sattuessa ja viiveen lyhentämisen sijoittamalla resurssit lähemmäs asiakkaita. Tämä jakelu sisältää myös joitakin sääntöjä siitä, miten resursseja voidaan käyttää yhdessä. (Google Cloud Platform.)

Pilvipalvelussa, ohjelmisto- ja laitteistotuotteista, tulee palveluita. Nämä palvelut tarjoavat pääsyn taustalla oleviin resursseihin. Käytettävissä olevien GCP-palvelujen luettelo on pitkä, ja se kasvaa jatkuvasti. Kun yritys liittää verkkosivustonsa tai -sovelluksensa GCP:hen, sovittaa se palvelut yhdistelmiksi, jotka tarjoavat sen tarvitsemaa infrastruktuuria. Tämän jälkeen lisätään koodi, jotta mahdolliset skenaariot voidaan luoda. (Google Cloud Platform.)

Joitakin resursseja voi käyttää millä tahansa muulla resurssilla eri alueiden ja alueiden välillä. Näihin maailmanlaajuisiin resursseihin sisältyvät esiasetetut levykuvat ja verkot. Joitakin resursseja voi käyttää vain resursseilla, jotka sijaitsevat samalla alueella. Nämä alueelliset resurssit sisältävät staattisia ulkoisia IP-osoitteita. Muita resursseja voi käyttää vain resursseilla, jotka sijaitsevat samassa vyöhykkeessä. Näitä alueellisia resursseja ovat virtuaalikoneiden-esiintymät, niiden tyypit ja levyt. (Google Cloud Platform.)

Seuraavassa kuvassa on esitetty globaalin laajuuden, alueiden ja vyöhykkeiden ja joidenkin niiden resurssien välinen suhde.



Kuva 5. Google Cloud Global Scope (Google Cloud 2018).

Toiminnan laajuus vaihtelee sen mukaan, millaisilla resursseilla työskennellään. Verkon luominen on esimerkiksi globaali operaatio, koska verkko on globaali resurssi, mutta IP-

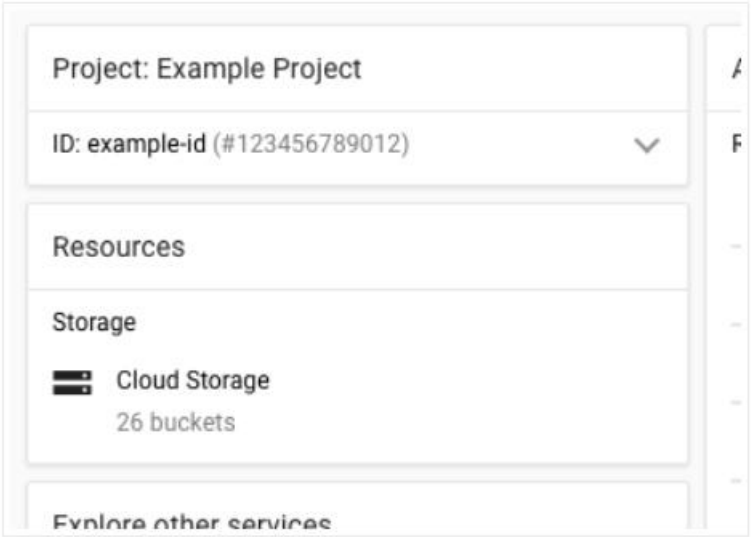
osoitteen varaaminen on alueellinen toiminta, koska osoite on alueellinen resurssi. (Google Cloud Platform.)

Kun GCP-sovellusten optimointi aloitetaan, on tärkeää ymmärtää, miten nämä alueet ja vyöhykkeet toimivat. Esimerkiksi, levyä ei haluta liittää yhden alueen tietokoneen toiseen alueeseen, vaikka voitaisiinkin, koska tällöin syntyisi viive, mikä antaisi erittäin huonon suorituskyvyn. Onneksi GCP on rakennettu niin, ettei se anna tehdä sitä, vaan levyt voidaan liittää vain samassa vyöhykkeessä oleviin tietokoneisiin. (Google Cloud Platform.)

Riippuen valitusta tietojenkäsittely- ja isännöintipalvelusta tarvittavasta itsehallinnan tasosta saatetaan joutua miettimään, miten ja missä resursseja jaetaan.

Kaikkien käytettyjen GCP-resurssien tulee kuulua projektiin. Projektia voi ajatella organisoivana kokonaisuutena siitä, mitä rakennetaan. Hanke koostuu asetuksista, käyttöoikeuksista ja muista metatiedoista, jotka kuvaavat asiakkaan sovelluksia. Yksittäisen projektin resurssit voivat työskennellä helposti, esimerkiksi viestimällä sisäisen verkon kautta alue- ja vyöhyke-sääntöjen mukaisesti. Resurssit, joita jokainen hanke sisältää, pysyvät erillään. Hankkeen rajojen yli voidaan liittää resursseja vain ulkoisen verkkoyhteyden kautta. (Google Cloud Platform.)

Jokaisella GCP-projektilla on projektin nimi, projekti id, jonka luodaan itse tai GCP luo ja projektinumero, jonka GCP luo. Kun käytetään GCP: tä, käytetään näitä tunnisteita tietyissä komentoriveissä ja API-puheluissa. Seuraavassa kuvassa näkyy projektin nimi, tunnus ja numero.



Kuva 6. Google Cloud Project esimerkki. (Google Coud 2018).

Jokainen projektitunnus on ainutlaatuinen GCP:ssä. Kerran luotu projekti voidaan poistaa, mutta sen tunnusta ei voi koskaan käyttää uudelleen.

Kun laskutus on käytössä, jokainen projekti liittyy yhteen laskutustiliin. Useiden projektien resurssien käyttö laskutetaan samalle tilille. (Google Cloud Platform.)

Projekti toimii nimitilana. Tämä tarkoittaa, että jokaisen projektin jokaisella resurssilla on oltava yksilöllinen nimi. Resurssien nimiä voidaan käyttää uudelleen, jos ne ovat eri projekteissa. Joidenkin resurssien nimien on oltava maailmanlaajuisesti ainutlaatuisia. (Google Cloud Platform.)

Google Cloud Platform -konsolissa on web-pohjainen graafinen käyttöliittymä, jota voidaan käyttää GCP-hankkeiden ja resurssien hallintaan. Kun käytetään GCP-konsolia, luodaan asiakkaalle uusi projekti tai valitaan olemassa oleva projekti ja käytetään sitä luomaan resursseja kyseisen projektin yhteydessä. Asiakas voi luoda useita projekteja ja näin käyttää projekteja erottamaan töitään millä tahansa tavalla mikä on kulloinkin tarpeen. Asiakas voi esimerkiksi käynnistää uuden projektin, jos hän haluaa varmistaa, että vain tietyt tiimin jäsenet voivat käyttää projektin resursseja, kun taas kaikki tiimin jäsenet voivat jatkaa resurssien käyttämistä toisessa projektissa. (Google Cloud Platform.)

Jos asiakas haluaa työskennellä pääteikkunassa, Google Cloud SDK tarjoaa gcloud-komentorivityökalun, jonka avulla voidaan käyttää tarvittavia komentoja. Gcloud-työkalua voidaan käyttää sekä kehitystyönkulun että GCP-resurssien hallintaan. (Google Cloud Platform.)

Cloud SDK sisältää asiakaskirjastoja, joiden avulla asiakas voi helposti luoda ja hallita resursseja. GCP-asiakaskirjastot paljastavat API:t kahdelle pääkäyttötarkoitukselle.

Sovellusliittymät mahdollistavat palvelujen käytön. Ne on optimoitu tuetuille kielille, kuten Node.js ja Python. Kirjastot suunnitellaan palveluketjujen ympärille, jolloin asiakas voi työskennellä palveluiden kanssa luonnollisemmin. Kirjastot tarjoavat myös avustajia todentamiseen ja valtuuttamiseen. (Google Cloud Platform.)

Admin-sovellusliittymät tarjoavat toiminnallisuutta resurssien hallintaan. Asiakas voi käyttää admin-sovellusliittymiä tai halutessaan luoda omia automaattisia työkaluja.

GCP antaa sinulle mahdollisuuden laskea ja hostata palveluita. Aasiakas voi valita seuraavista vaihtoehdoista: työskennellä palvelimattomassa ympäristössä tai käyttää hallittua sovellusalustaa. Hyödyntää säiliöteknologiaa, jolloin asiakas saa paljon joustavuutta. Asiaka voi rakentaa oman pilvipohjaisen infrastruktuuri, millä on eniten hallintaa ja joustavuutta. (Google Cloud Platform.)

Google-pilvitoiminnot, GCP:n toiminto palveluna (FaaS) tarjoavaa palvelittoman suoritusympäristön pilvipalvelujen rakentamiseen ja yhdistämiseen. Cloud Functions -toiminnolla asiakas voi kirjoittaa yksinkertaisia, yksitoimisia toimintoja, jotka liitetään pilvi-infrastruktuurin ja palveluiden esiin tuomiin tapahtumiin. Cloud-toiminto toimii, kun katselutapahtuma on nostettu. Koodi suoritetaan täysin hallinnoidussa ympäristössä. Asiakkaan ei tarvitse järjestää mitään infrastruktuuria tai huolehtia palvelimen hallinnasta. (Google Cloud Platform.)

Asiakas voi kirjoittaa Cloud Functions -ohjelmaa JavaScriptin avulla ja suorittaa ne GCP:ssä Node.js v6.11.5 -ympäristössä. Asiakas voi käyttää Cloud Function -toimintoa kaikissa standardeissa Node.js-runtime-ohjelmissa, mikä helpottaa siirrettävyyttä ja paikallista testausta. (Google Cloud Platform.)

Google App Engine on GCP:n alusta palveluna (PaaS). App Enginen avulla Google käsittelee suurimman osan resurssien hallinnasta. Jos asiakkaan sovellus edellyttää esimerkiksi enemmän tietojenkäsittelyresursseja, koska asiakkaan verkkosivusto liikenne kasvaa, niin Google skaalaa järjestelmän automaattisesti, jotta ne voisivat tarjota resursseja. (Google Cloud Platform.)

Konttipohjaisen tietojenkäsittelyn avulla asiakas voi keskittyä sovelluskoodiin sen sijaan, että käyttäjä keskittyisi hosting-ympäristöihin. Google Kubernetes -moottori, GCP: n kontit palveluna (CaaS), on rakennettu avoimen lähdekoodin Kubernetes-järjestelmään, joka tarjoaa joustavuuden paikallisissa tai hybridilevyissä GCP: n julkisen pilvipalvelujen lisäksi. (Google Cloud Platform.)

GCP: n hallitsematon laskentapalvelu on Google Compute Engine. Asiakas voi ajatella Compute Engine -palvelun tarjoavan infrastruktuuria palveluna (IaaS), koska järjestelmä tarjoaa vankan tietotekniikan infrastruktuurin, mutta asiakkaan on valittava ja määritettävä käytettävät alustan komponentit. Compute Engine -sovelluksen avulla on asiakkaan tehtävä määrittää, hallita ja seurata järjestelmiä. Google varmistaa, että resurssit ovat käytettävissä, luotettavia ja valmiita käyttämään niitä, mutta niiden

tehtävänä on tarjota ja hallita niitä. Tässä etuna on se, että järjestelmät ovat täysin hallinnassa ja joustavuus rajoittamatonta. (Google Cloud Platform.)

Asiakkaan ei tarvitse tarttua vain yhteen tietotekniikkapalveluun. Asiakas voi esimerkiksi yhdistää App Engine- ja Compute Engine -tuotteet, voidakseen hyödyntää kunkin palvelun ominaisuuksia ja etuja. (Google Cloud Platform.)

Vaikka App Engine hallinnoi verkottumista ja Kubernetes Engine käyttää Kubernetes-mallia, Compute Engine tarjoaa joukon verkkopalveluja. Nämä palvelut auttavat lataamaan tasapainoisen liikenteen resurssien välillä, luomaan DNS-tietueita ja yhdistämään nykyisen verkoston Googlen verkkoon. (Google Cloud Platform.)

GCP Cloud AI tarjoaa erilaisia tehokkaita koneen oppimispalveluja. Asiakas voi käyttää API-ohjelmia, jotka tarjoavat valmiiksi koulutettuja malleja, jotka on optimoitu tietyille sovelluksille, tai rakentaa ja kouluttaa omia laajamittaisia, kehittyneitä malleja käyttämällä hallittua TensorFlow-kehystä. (Google Cloud Platform.)

6 PILVIPALVELUIDEN TIETOTURVA OMINAISUUKSIA

Pilvipalveluiden turvallisuus, koostuu joukosta käytäntöjä, ohjauksia, menettelyjä ja teknologioita, jotka toimivat yhdessä pilvipohjaisten järjestelmien, tietojen ja infrastruktuurin suojaamiseksi. Nämä turvatoimenpiteet on määritetty suojaamaan tietoja, tukemaan sääntöjen noudattamista ja suojaamaan asiakkaiden yksityisyyttä sekä asettamaan todennussäännöt yksittäisille käyttäjille ja laitteille. Suodatusliikenteen saannin varmistamisesta pilvensuojaus voidaan määrittää liiketoiminnan tarpeisiin. Ja koska nämä säännöt voidaan konfiguroida ja hallita yhdessä paikassa, hallinnon yleiskustannukset pienenevät ja IT-tiimit voivat keskittyä muihin liiketoiminta-alueisiin. (Forcepoint 2019.)

Pilvipalvelun toimitus riippuu yksittäisestä pilvipalveluntarjoajasta tai pilvipalveluratkaisuista. Yrityksen omistajalla ja ratkaisun tarjoajalla tulisi kuitenkin olla yhteinen vastuu pilvipalveluprosessien toteuttamisesta.

Yrityksille, jotka siirtyvät pilviin, luotettava tietoturva on välttämätöntä. Turvallisuusuhat kehittyvät jatkuvasti ja pilvipalvelut ovat yhtä vaarassa kuin ympäristö. Tästä syystä on välttämätöntä työskennellä pilvipalvelujen tarjoajan kanssa, joka tarjoaa parhaan mahdollisen tietoturvan, joka on räätälöity infrastruktuuriin. (Forcepoint 2019.)

Yhä useammat organisaatiot ymmärtävät monia liiketoiminnallisia etuja, joita IT palveluiden siirtäminen pilveen tuo. On kuitenkin olennaista, että järjestöt luottavat pilvipalvelujen tietoturvaan ja että kaikki tiedot, järjestelmät ja sovellukset ovat suojattuja tietojen varkauksilta, vuodoilta, korruptiolta ja poistamisilta. (Forcepoint 2019.)

Kaikki pilvimallit ovat alttiita uhille. Tietotekniikan osastot ovat luonnollisesti varovaisia siirtämään lähetyskriittisiä järjestelmiä pilviin. On olennaista, että käytössä on oikeat turvasäännökset. Cloud Security tarjoaa kaikki perinteisen IT-tietoturvan toiminnot ja mahdollistaa yritysten hyödyntää pilvipalvelun monia etuja ja samalla varmistaa, että tietosuoja- ja vaatimustenmukaisuusvaatimukset täyttyvät. (Forcepoint 2019.)

Lähes kaikki pilvipalvelujen tarjoajat tuottavat jonkin näköisiä tietoturvaratkaisuja. Tarkoituksena on seuraavaksi käydä läpi näiden kolmen edellä mainitun pilvipalvelun tietoturvaominaisuuksia.

6.1 Microsoft Azuren ominaisuuksia

Microsoft Azuren sisäänrakennetut ominaisuudet on järjestetty kuuteen toiminnalliseen alueeseen: Operations, Applications, Storage, Networking, Compute ja Identity.

Microsoft Azure käyttää kehittynyttä koneellista oppimista. Azuren Unified Security Management ja Advanced Threat Protection pitävät huolta asiakkaan tietoturvasta olivat ne sitten pilvessä tai omissa palvelimissa. Kaikki Azuren palvelut ovat suunniteltu niin että niillä on monen kerroksen suojaus. (Microsoft Azure Introduction to Azure Security)

Azuren Security Center avulla seuraat ja hallitset helposti tietoturvaasi. Tietoturvaa parantaa myös Adaptive Threat Protection ja Intelligent Threat Detection and Response, mitkä helpottavat tietoruvatason seuraamista. Security and Audit -ratkaisu tarjoaa kattavan näkymän organisaation tietoturva-asentoon, jossa on sisäänrakennettuja hakukyselyjä huomionarvoisista ongelmista. Tietoturva- ja auditointipaneelissa näkyvät kaikki asiat, jotka liittyvät Azure Monitorin lokien tietoturvaan. Se tarjoaa korkean tason käsityksen tietokoneesi suojaustilasta. Se sisältää myös mahdollisuuden tarkastella kaikkia viimeisten 24 tunnin, 7 päivän tai minkä tahansa muun mukautetun ajanjakson tapahtumia. (Microsoft Azure Introduction to Azure Security)

Application Insights on laajennettava Application Performance Managementin (APM) palvelu web-kehittäjille. Application Insights sovelluksen avulla voidaan seurata live-sovelluksia ja tunnistaa automaattisesti suorituskyvyn poikkeamat. Se sisältää tehokkaita analyysityökaluja, joiden avulla voit diagnosoida ongelmat ja ymmärtää, mitä käyttäjät todella tekevät sovellusten kanssa. Se valvoo asiakkaan sovellusta koko ajan, kun se on käynnissä sekä testauksen aikana että sen julkaisemisen tai käyttöönoton jälkeen. (Microsoft Azure Introduction to Azure Security)

Sovellusnäkymät luovat kaavioita ja taulukoita, jotka näyttävät asiakkaalle esimerkiksi, minä päivinä on eniten käyttäjiä ja kuinka hyvin sitä palvelevat ulkoiset palvelut, joista se on riippuvainen. (Microsoft Azure Introduction to Azure Security)

Azure Monitor tarjoaa visualisointia, kyselyä, reititystä, hälytystä, automaattista skaalaa ja automaatiota sekä Azure-infrastruktuurista (Activity Log) että kustakin yksittäisestä Azure-resurssista (Diagnostic Logs). Asiakas voi käyttää Azure Monitoria hälyttämään tietoturvaan liittyvistä tapahtumista, jotka on luotu Azure-lokeihin. (Microsoft Azure Introduction to Azure Security)

Azure Monitor Logs Tarjoaa IT-hallintaratkaisun sekä paikan päällä että kolmannen osapuolen pilvipohjaiseen infrastruktuuriin (kuten AWS) Azure-resurssien lisäksi. Azure Monitorin tietoja voidaan ohjata suoraan Azure Monitorin lokeihin, jotta asiakas voi nähdä koko ympäristöä koskevat tiedot ja lokit yhdessä paikassa. (Microsoft Azure Introduction to Azure Security)

Azure Application Gatewayn web-sovelluksen palomuuri (WAF) auttaa suojaamaan web-sovelluksia tavallisilta web-pohjaisilta hyökkäyksiltä, kuten SQL-injektiolta, sivustojen välisten komentosarjojen hyökkäyksiltä ja istuntojen kaappaukselta. Se on esiasennettu tunnistamaan uhat, jotka ovat Open Web Application Security Projectin (OWASP) kymmenen tunneitumman uhan listalla. (Microsoft Azure Introduction to Azure Security)

Sovelluspalvelun todennus tai valtuutus on ominaisuus, jonka avulla sovellukset voi kirjautua käyttätileihin, jotta asiakkaan ei tarvitse muuttaa koodia sovelluksen taustalla. Se tarjoaa helpon tavan suojata sovelluksen ja käyttää käyttäjätietoja

Asiakas voi suojata tallennustilinsä RBAC:llä(Role-Based Access Control).Pääsyn rajoittaminen käyttöoikeuksien mukaan on elintärkeää yrityksille, jotka haluavat vahvistaa tietoturva käytäntöjään. Nämä käyttöoikeudet annetaan antamalla asianmukainen RBAC-rooli ryhmille ja sovelluksille tietyllä laajuudella. Voidaan käyttää sisäänrakennettuja RBAC-rooleja, kuten tallennustilien avustajaa, määrittämään käyttäjille käyttöoikeudet. Pääsy Azure Resource Manager mallia käyttävään tallennustiliin voidaan tallentaa RBAC:n avulla. Kaikki data mitä Azureen laittaa on suojattua ja enkryptattua ja Azuren koneellinen oppiminen varoittaa mahdollisista tietoturva uhista. (Microsoft Azure Introduction to Azure Security)

Verkon käyttöoikeuksien hallinta edustaa verkon turvallisuuden ydintä. Verkkokäytön valvonnan tavoitteena on varmistaa, että virtuaalikoneet ja -palvelut ovat käytettävissä vain käyttäjille ja laitteille, joihin haluat niiden saatavuuden.

Verkkoturvallisuusryhmä (NSG) on perusvalmis pakettisuodatuksen palomuuri, jonka avulla voidaan hallita 5-kerroksisen pääsy. NSG:t eivät tarjoa sovelluskerroksen tarkastusta tai todennettuja pääsynhallintoja. Niitä voidaan käyttää valvomaan liikennettä, joka liikkuu aliverkkojen välillä Azure-virtuaaliverkossa ja liikennettä Azure-virtuaaliverkon ja Internetin välillä. (Microsoft Azure Introduction to Azure Security)

Kyky hallita reitityskäyttäytymistä Azure Virtual Networksissä on kriittinen verkon suojaus ja käyttöoikeuksien hallinta. Jos asiakas haluaa esimerkiksi varmistaa, että kaikki Azure Virtual Network -liikenne ja sen kautta kulkeva liikenne kulkee kyseisen virtuaalisen suojauslaitteen läpi, täytyy pystyä ohjaamaan ja mukauttamaan reitityskäyttäytymistä. Tämä voidaan tehdä tämän määrittämällä käyttäjän määrittelemät reitit Azuressa. (Microsoft Azure Introduction to Azure Security)

Azure Active Directory, kattava identiteetti- ja pääsynhallintapilven ratkaisu, auttaa varmistamaan pääsyn sivuston ja pilven sovelluksissa oleviin tietoihin ja yksinkertaistaa käyttäjien ja ryhmien hallintaa. Se yhdistää keskeiset hakemistopalvelut, kehittyneen identiteetin hallinnan, tietoturvan ja sovellusten käyttöoikeuksien hallinnan ja tekee kehittäjille helpon tavan rakentaa politiikkaan perustuvaa identiteetinhallintaa sovelluksiinsa. Azure Active Directoryn voidaan parantaa lisäämällä maksullisia ominaisuuksia käyttämällä Azure Active Directory Basic, Premium P1 ja Premium P2 -versioita. (Microsoft Azure Introduction to Azure Security)

Azure IaaSin avulla asiakas voi käyttää antimalware-ohjelmistoja tietoturvatoimittajilta, kuten Microsoftilta, Symantecilta, Trend Microltä, McAfeelta ja Kasperskyltä, suojaamaan virtuaalikoneita haittaohjelmilta, mainosohjelmilta ja muilta uhilta. Microsoft Antimalware Azure Cloud -palveluille ja virtuaalikoneille on suojaus, joka auttaa tunnistamaan ja poistamaan viruksia, vakoiluohjelmia ja muita haittaohjelmia. Microsoft Antimalware tarjoaa konfiguroitavia hälytyksiä, kun tunnetut haitalliset tai ei-toivotut ohjelmistot yrittävät asentaa itsensä tai käyttää asiakkaan Azure-järjestelmiä. Microsoft Antimalware voidaan ottaa käyttöön myös Azure Security Centerin avulla. (Microsoft Azure Introduction to Azure Security)

6.2 Amazon Web services ominaisuuksia

Kun asiakas isännöi sovellusta pilvessä, on hän sitoutunut jakamaan vastuut AWS:n kanssa. Amazon Web Services Securityn tehtävänä on huolehtia isäntäkäyttöjärjestelmistä, visualisointikerroksesta, verkosta ja fyysisestä suojauksesta. (Nitheesh Poojary 2015).

Käyttämällä Identity and Access Management (IAM) -toimintoa asiakas voi luoda käyttäjiä, ryhmiä ja rooleja. Asiakas käyttää oikeuksia sallia ja kieltää niiden

käyttöoikeudet AWS-resursseihin, kuten EC2, RDS ja VPC. IAM: n avulla. Asiakas voi myöntää ainutkertaiset käyttöoikeudet jokaiselle AWS-tilin käyttäjälle, mikä mahdollistaa yksilöllisen pääsyn vain tarvittaviin AWS-palveluihin ja resursseihin. Kun IAM Mutifactor Authentication on käytössä, käyttäjää, joka yrittää käyttää AWS-resurssia, pyydetään antamaan normaali todennus (käyttäjätunnus ja salasana), mutta myös autentikointikoodi, joka on käytettävissä vain MFA-konfiguroidun laitteen kautta. IAM:n avulla asiakas voi myöntää työntekijöille ja sovelluksille AWS-hallintakonsolin ja AWS-palvelun API: n. IAM on myös yhteensopiva nykyisen Active Directoryn kanssa. (Nitheesh Poojary 2015).

Amazonin VPC:t (Virtual Private Cloud) mahdollistavat laskennallisten resurssien, kuten EC2-esiintymien ja RDS-sovellusten, tarjoamisen erillisissä virtuaaliverkkoissa. VPC:t antavat täydellisen hallinnan kaikista saapuvista ja lähtevistä verkkoliikenne tapahtumista. Asiakas voi suojata sovellukset VPC: iden avulla rajoittamalla tarvittaessa Internet-yhteyttä. Virtuaalisen yksityisverkon (VPN) yhteyksien avulla asiakas voi kytkeä palvelimella olevia palvelimia suoraan pilvipohjaiseen VPC:hen ohittaen julkiset verkot. (Nitheesh Poojary 2015).

Suojausryhmiä käyttämällä asiakas voi luoda palomuurin sääntöjä, jotka ohjaavat saapuvaa ja lähtevää liikennettä. Asiakas voi rajoittaa liikennettä protokollatyypin (TCP, UDP, ICMP), IP-osoitteen ja portin mukaan. (Nitheesh Poojary 2015).

Access Control Lists (ACL) toimivat aliverkon tasolla. Verkon ACL: t voivat olla erityisen hyödyllisiä DDOS-hyökkäysten ehkäisyssä. AWS tarjoaa myös tietojen salausta EBS-volyymeille, S3-kauhoille ja relaatiotietokantapalvelulle (RDS) ja Glacier-tietovarastoille. (Nitheesh Poojary 2015).

RDS luo SSL-sertifikaatin kullekin DB-instanssille. Kun salattu yhteys on muodostettu, DB-instanssin ja sovelluksen välillä siirretyt tiedot salataan siirron aikana. Amazon S3: n palvelinpuolen salaus käyttää yhtä voimakkaimmista käytettävissä olevista salauksen salauksista - 256-bittinen Advanced Encryption Standard (AES-256). (Nitheesh Poojary 2015).

Asiakas voi käyttää AWS Direct Connectia luomaan yksityisen virtuaalisen käyttöliittymän oman verkon ja Amazon Virtual Private Cloudin välillä. Direct Connect tarjoaa yksityisen ja suojatun laajakaistayhteyden. (Nitheesh Poojary 2015).

CloudTrail tarjoaa historiaa kaikista API-puheluista, jotka on tehty tilien resursseja vastaan, mukaan lukien AWS Management Console-, SDK- ja komentorivityökalujen kautta tehdyt API-puhelut. (Nitheesh Poojary 2015).

AWS Trusted Advisor tarkastaa AWS-ympäristön ja antaa suosituksia säästää rahaa, parantaa järjestelmän suorituskykyä ja luotettavuutta tai sulkea tietoturvaa.

Jopa ilman päivitettyä maksullista tukisuunnitelmaa, Trusted Advisor varoittaa asiakasta heikkouksista, kuten turvallisuusryhmistä, jotka sallivat rajoittamattoman pääsyn (0.0.0.0/0) tiettyihin satamiin tai S3-kauhoihin, joissa on avoimet käyttöoikeudet. Trusted Advisor voi tarjota erittäin tehokkaan yhteenvedon yleisestä Amazon Web Services -turvallisuusprofiilista. (Nitheesh Poojary 2015).

6.3 Google Cloud Platformin ominaisuuksia

Google-tietokeskuksissa on kerrostettu tietoturvamalli, mukaan lukien suojat, kuten räätälöityjä elektronisia kortteja, hälytyksiä, ajoneuvon pääsyrajoituksia, kehä-aidat, metalli-ilmaisimet ja biometriset tiedot. Tietokeskuksen lattia sisältää lasersäteen tunkeutumisen havaitsemisen. (Google Cloud)

Googlen tietokeskuksia valvotaan vuorokauden ympäri korkean resoluution sisä- ja ulkopuolisilla kameroilla, jotka voivat havaita ja seurata tunkeilijoita. Access-lokit, aktiviteettitiedot ja kameramateriaalit tarkistetaan, jos jotain tapahtuu. Tietokeskuksia valvotaan myös rutiininomaisesti kokeneilla turvatarkastajilla, jotka ovat läpikäyneet tiukat taustan tarkistukset ja koulutuksen. (Google Cloud)

Googlella käytetään kymmeniä tuhansia identtisiä, räätälöityjä palvelimia. Google on rakentanut kaiken laitteistosta ja verkottumisesta mukautettuun Linux-ohjelmistopinoon. Homogeenisuus yhdistettynä koko pinon omistukseen vähentää merkittävästi turvallisuusjalanjälkeä ja mahdollistaa nopeamman reagoinnin uhkiin. (Google Cloud)

Ainoa tapa suojata palvelimen käynnistysprosessi on turvata se sellaisella kokonaisuudella, jonka voidaan luottaa käyttäytyvän aina odotetulla tavalla. Googlella on tarkoitus rakentaa Titan-niminen tietoturvasiru tämän luottamuksen juuren aikaansaamiseksi. Titan mahdollistaa järjestelmän laiteohjelmiston ja ohjelmistokomponenttien tarkistamisen ja luo vahvan, laitteistoon perustuvan järjestelmän identiteetin. (Google Cloud)

Googlella on valvontaa ja käytäntöjä, joilla suojataan asiakastietojen turvallisuutta. Google-sovelluksen ja tallennuspinon kerrokset edellyttävät, että muista komponenteista tulevat pyynnöt todennetaan ja hyväksytään. Tuotantosovellusten hallinnon insinöörien pääsyä tuotantoympäristöihin ohjataan myös. Keskitetyn ryhmä- ja roolinhallintajärjestelmän avulla määritellään ja ohjataan insinöörien pääsyä tuotantopalveluihin käyttämällä turvallisuusprotokollaa, joka todentaa insinöörit käyttämällä lyhytaikaisia henkilökohtaisia julkisia avaimia koskevia sertifikaatteja. Henkilökohtaisten varmenteiden myöntämistä valvoo puolestaan kaksitekijätodennus. (Google Cloud)

Kun Googlen järjestelmistä poistutaan, asiakastietoja sisältäviä kiintolevyjä käsitellään ennen tietojen poistamista Googlen tiloista. Ensinnäkin valtuutetut henkilöt pyyhkivät loogisesti levyt Google Security Teamin hyväksymän prosessin avulla. Sitten toinen valtuutettu henkilö suorittaa toisen tarkastuksen varmistaakseen, että levy on pyyhitty onnistuneesti. Nämä poistotiedot kirjataan taajuusmuuttajan sarjanumeroon seurantaan. Lopuksi poistettu asema vapautetaan varastoon uudelleenkäyttöä ja uudelleensijoittamista varten. Jos asemaa ei voi poistaa laitteiston vian vuoksi, se tallennetaan turvallisesti, kunnes se voidaan fyysisesti tuhota. Kukin laitos tarkastetaan viikoittain levynpoistopolitiikan noudattamisen valvomiseksi. (Google Cloud)

Kaikki Googlen tuotteet, mukaan lukien Cloud Platform, on rakennettu turvallisuudella keskeisenä suunnittelun ja kehittämisvaatimuksena. Lisäksi Googlen sivustojen luotettavuuden suunnitteluryhmät valvovat alustan järjestelmien toimintaa, jotta varmistetaan korkea saatavuus ja estetään käyttöympäristön resurssien väärinkäyttö. Tuotekohtaiset suojausominaisuudet on kuvattu jokaisen tuotteen dokumentaatiossa, mutta kaikki tilaavat tietyt laajuiset ominaisuudet. (Google Cloud)

Kaikki palvelut hoidetaan suojatulla maailmanlaajuisella API-yhdyskäytäväinfrastruktuurilla. Tämä API-palveleva infrastruktuuri on käytettävissä vain salattujen SSL / TLS-kanavien kautta, ja jokaisen pyynnön on sisällettävä aikarajoitettu tunnistusmerkki, joka on luotu ihmisen kirjautumisen tai yksityisten avainpohjaisten salaisuuksien kautta yllä kuvatun autentikointijärjestelmän kautta. (Google Cloud)

Kaikkia Google Cloud Platform -resurssien käyttöoikeuksia säännellään samalla vahvalla todennetulla infrastruktuurilla, joka käyttää muita Google-palveluita. Tämä tarkoittaa sitä, että voidaan käyttää olemassa olevia Google-tilejä tai määrittää säännellyn Googlen hallinnoiman verkkotunnuksen. Käyttäjien hallintaan käytettävissä

olevia ominaisuuksia ovat salasanapolitiikka, pakotettu 2-tekijän todennus ja uudet innovaatiot todentamisen valvomiseksi laitteiston suojausnäppäinten muodossa. (Google Cloud).

Kaikki alustan API-pyynnöt kirjataan, kuten web-pyynnöt, tallennustilan kauhan käyttö ja käyttäjätilin käyttöoikeudet. Cloud Platform -työkalujen avulla asiakas voi lukea Compute Engine, App Engine, BigQuery, Cloud SQL, Deployment Manager, Cloud VPN ja Cloud Storage sovellusten lokeja. (Google Cloud)

Cloud Platform -palvelut salaavat aina asiakkaan sisällön, joka on tallennettu lepotilassa, muutamalla pienellä poikkeuksella. Salaus on automaattista, eikä asiakkaan toimia tarvita. Käytetään yhtä tai useampaa salausmekanismia. Esimerkiksi kaikki pysyviin levyihin tallennetut uudet tiedot salataan 256-bittisen Advanced Encryption Standardin (AES-256) mukaisesti, ja jokainen salausavain on itse salattu säännöllisesti kiertyvällä pääavaimilla. Monet Googlen tuotannon palvelut, kuten Gmail ja Googlen omat yritystiedot, käyttävät samaa salaus- ja avainhallintapolitiikkaa, salaustietokantoja ja luottamuksen juuria, joita käytetään Google Cloud Platformissa. (Google Cloud)

Koska Google on yhteydessä useimpiin Internet-palveluntarjoajiin maailmassa, Googlen maailmanlaajuinen verkko auttaa parantamaan kauttakulkuneuvojen tietoturvaa rajoittamalla hyppyjä julkisessa Internetissä. Cloud Interconnectin ja hallinnoidun VPN:n avulla voidaan luoda salattuja kanavia omassa IP-ympäristössä tiloissa ja Googlen verkossa. Tämän avulla voidaan pitää tapaukset täysin erillään julkisesta Internetistä, mutta ne ovat edelleen käytettävissä omalta yksityiseltä infrastruktuurilta. (Google Cloud)

Googlen tunkeutumisen havaitseminen edellyttää Googlen hyökkäyspinnan koon ja kokoonpanon tiukkaa valvontaa ennaltaehkäisevien toimenpiteiden avulla, käyttäen älykkäitä havaitsemisohjaimia datan syöttöpisteissä ja käyttämällä tekniikoita, jotka korjaavat automaattisesti tietyt vaaralliset tilanteet. (Google Cloud)

Cloud Security Scanner auttaa App Engine -kehittäjiä tunnistamaan yleisimmät haavoittuvuudet, erityisesti sivustojen väliset komentosarjat (XSS) sovelluksissaan.

Cloud Platform ja Google-infrastruktuuri on sertifioitu noudattamaan yhä useampia vaatimustenmukaisuusstandardeja ja -ohjauksia, ja niissä tehdään useita riippumattomia kolmannen osapuolen tarkastuksia, joilla testataan tietoturvallisuutta, yksityisyyttä ja tietoturvaa.(Google Cloud)

7 POHDINTA

Opinnäytetyön tarkoituksena oli käydä läpi, mitä pilvipalvelut ovat, millaisia palveluja ne tarjoavat ja onko niiden tietoturva riittävää. Pilvipalvelut ovat oleellinen osa nykypäivän yrityksiä, mutta uskon, että monille pilvipalvelut se, mitä niillä voidaan tehdä ei ole vielä selkeää. Tämän opinnäytetyön luettua pystytään selkeästi ymmärtämään mitä pilvipalvelut ovat, ja mitä kaikkea niillä voidaan tehdä.

Monia mietityttää siirtyminen pilvipalveluihin niiden turvallisuuden takia. Nykypäivän pilvipalvelut ovat kuitenkin juuri niin suojattuja kuin asiakas itse ymmärtää niistä tehdä. Kaikki pilvipalvelut tarjoavat asiakkailleen kattavan määrän tietoturvatyökaluja ja ominaisuuksia, joita käyttämällä tiedot ovat yhtä turvassa, kuin ne olisivat yrityksen omalla palvelimella.

Pilvipalvelut ovat mielestäni tärkeä osa yrityksen IT-infrastuktuuria niin nykypäivänä kuin tulevaisuudessakin. Pilvipalvelut tulevat vielä kehittymään tulevien vuosien aikana, niin että ne ovat pakollinen osa lähes jokaisen yrityksen IT-infrastruktuuria. Pilvipalvelut toimittavat paljon ominaisuuksia ja mahdollisuuksia, jotka muuten olisivat yritykselle kalliita ja niitä varten pitäisi palkata lisää henkilökuntaa ylläpitämään palveluita. Pilvipalvelut sen sijaan tarjoavat palvelut siten että ne on helpommin hallittavissa ja pilvipalvelut skaalautuvat helpommin, jolloin jos asiakas tarvitsee esimerkiksi lisää tilaa, ei hänen tarvitse ostaa kalliita laitteita vaan tilaa voidaan ostaa pilvipalveluista lisää halvemmalla.

Opinnäytetyössä käytetty aineisto tarjoaa selkeän kuvan siitä, mitä pilvipalvelut pystyvät tarjoamaan yrityksille ja yksityishenkilöille, sekä kuinka luotettavia ne oikeasti ovat. Aineisto tarjoaa kattavan tarjouksen pilvipalveluiden ominaisuuksista niin tavallisessa kuin yrityskäytössä. Aineistosta tulee myös selvästi ilmi pilvipalveluiden tietoturvan taso.

Pilvipalvelut ovat kehittymässä niin suurta vauhtia, että jos niistä haluaisi pysyä aina ajan tasalla pitäisi niistä lukea jotain uutta lähes joka viikko. Vaikka opinnäytetyössä käytetty aineisto onkin kattava ja tarjoaa selkeän kuvan pilvipalveluista ei voi silti varmaksi sanoa miltä pilvipalvelut tulevat näyttämään tulevaisuudessa.

LÄHTEET

Access Alto 2017. History of Cloud Computing. Viitattu 12.4.2019 https://www.theaccessgroup.com/hosting/resources/our-blog/history-of-cloud-computing/.

Barr J. 2014. Hue – A Web User Interface for Analyzing Data With Elastic MapReduce. Viitattu 18.4.2019 https://aws.amazon.com/blogs/aws/hue-web-ui-for-emr/.

Forcepoint 2019. What is Cloud Security? Viitattu 17.4.2019 https://www.forcepoint.com/cyber-edu/cloud-security.

Frank B. 2014. The pros and cons of cloud computing. Viitattu 16.4.2019 https://www.ibm.com/blogs/cloud-computing/2014/05/13/the-pros-and-cons-of-cloud-computing/.

Google Cloud 2019. Google Security Overview. Viitattu 18.4.2019 https://cloud.google.com/security/overview/.

Google Cloud Platform 2018. Google Cloud Platform Overview. Viitattu 17.4.2019 https://cloud.google.com/docs/overview/.

Graham K. 2017. DevOps and PaaS. Viitattu 16.4.2019 https://codematters.online/devops-paas/.

Hanselman S. 2019. Get Started With Azure Portal. Viitattu 18.4.2019 https://azure.microsoft.com/en-us/resources/videos/get-started-with-azure-portal/.

Heino P. 2010. Talentum media Oy Pilvipalvelut s51-57.

Knorr E. 2018. What is Cloud computing? Everything you need to know now. Viitattu 15.4.2019 https://www.infoworld.com/article/2683784/what-is-cloud-computing.html.

McSpirit M. 2019. Start with a secure foundation. Viitattu 16.4.2019 https://azure.microsoft.com/en-us/overview/security/.

Mell Peter, Grance Tim 2011. The NIST Definition of Cloud Computing. Viitattu 12.4.2019 https://csrc.nist.gov/publications/detail/sp/800-145/final.

Microsoft Azure 2019. Introduction to Azure Security. Viitattu 17.4.2019 https://docs.microsoft.com/en-us/azure/security/azure-security.

Microsoft Azure 2019. What is Hybrid Cloud? Viitattu 16.4.2019 https://azure.microsoft.com/en-in/overview/what-is-hybrid-cloud-computing/.

Microsoft Azure 2019. What is Private Cloud? Viitattu 16.4.2019 https://azure.microsoft.com/en-us/overview/what-is-a-private-cloud/.

Microsoft Azure 2019. What is Public Cloud? Viitattu 16.4.2019 https://azure.microsoft.com/en-us/overview/what-is-a-public-cloud/.

NIST 2008. NIST General Information. Viitattu 15.4.2019 https://www.nist.gov/director/pao/nist-general-information.

Poojary N. 2015. Amazon Web Services Security: Using the Built-in Features. Viitattu 18.4.2019 https://cloudacademy.com/blog/amazon-web-services-security/.

Rouse M. 2017. Amazon Web Services (AWS). Viitattu 17.4.2019 https://searchaws.techtarget.com/definition/Amazon-Web-Services.

Shortslef N. 2019. Microsoft Azure explained: what it is and why it matters. Viitattu 16.4.2019 https://ccbtechnology.com/what-microsoft-azure-is-and-why-it-matters/.

Viswanathan P. 2018. Pros and cons of cloud computing. Viitattu 16.4.2019 https://www.lifewire.com/cloud-computing-explained-2373125.