Kalle Vettenranta

KÄYTTÄJÄNHALLINTA PILVIPALVELUISSA

Tietojenkäsittelyn koulutusohjelma

2016

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

KÄYTTÄJÄHALLINTA PILVIPALVELUISSA

Vettenranta, Kalle
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tammikuu 2016
Ohjaaja: Grönholm, Jukka
Sivumäärä: 34
Liitteitä:

Asiasanat: Käyttäjähallinta, Pilvipalvelut, Active Directory, Jump Cloud

---

Työssä esiteltiin mitä ovat pilvipalvelut ja käyttäjähallinta. Työssä selvitettiin mitä niiden kehitys on ollut ja pohdittiin myös vähän tulevaisuutta. Työssä pohdittiin myös miksi yritys haluaisi käyttää kyseisiä palveluita.

Työssä määriteltiin mitä ovat pilvipalvelut. Käytiin läpi miksi yritykset haluaisivat niitä käyttää. Työssä määriteltiin mitä ovat pilvipalveluntarjoajat ja pilvitoimijat. Työssä esiteltiin, miten pilvipalvelut jaotellaan niiden arkkitehtuurin tai niiden toimintaympäristön kautta.

Työssä käytiin läpi mitä käyttäjähallinta on ollut ja mitä se on nykyään. Työssä tuotiin esille miten käyttäjähallinto on läheisesti yhteydessä myös tietoturvaan. Käytiin läpi Googlen ja Facebookin tarjoamia autentikoiti palveluja.

Opinnäytetyö etenee pilvipalveluista käyttäjähallintaan. Niiden jälkeen käytiin läpi pilvipalveluiden yleisiä ongelmia ja tietoturvaa. käsiteltiin miten erilaisia autentikointi ratkaisuja voidaan yhdistellä luomaan turvatumpia kirjautumisia. Viimeisimpänä aiheena pohdittiin vähän tulevaisuutta.

USER MANAGEMENT AND CLOUD SERVICES

Vettenranta, Kalle
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information handling
January 2016
Supervisor: Grönholm, Jukka
Number of pages: 34
Appendices:

Keywords: user management, cloud services, Active Directory, Jump Cloud

---

The purpose of this thesis was to introduce the reader to the world of cloud services and user management. The beginning and evolution of these services was a point in the thesis. The thesis was written mostly for businesses.

What is the definition of cloud based services was defined in this thesis. Why businesses would want to use them was covered. What is the definition of cloud based service provider and how they differ from cloud operatives. Cloud services and how they are divided according to their architecture and their operational environment.

User management and its birth was one of the key points in this thesis. It was introduced, what computing was before user management and what it has become. In the thesis it was also noted that user management is also closely related to security. Facebook's and Google's new user authentication services were noted in the thesis.

Cloud based services were introduced first. After that, user management, then some difficulties these services might bring. And lastly there was some security and the future.

SISÄLLYS

1 JOHDANTO

Tässä työssä käsitellään pilvipalveluiden ja käyttäjähallinnan ratkaisuja. Käsitellään pilvipalveluiden hyödyntämisessä sovellettavia käyttäjähallinnan periaatteita. Näitä asioita tarkastellaan lähinnä yritysten näkökannasta.

Pilvipalvelut ovat nykyaikaisia palveluita, eikä niitä välttämättä osata vielä arvostaa tai käyttää niiden potentiaalin mukaisesti. Käsitellään mitä asioita käyttäjän pitäisi huomioida käyttäessään palveluita. Näitä asioita ovat esimerkiksi tietoturva asiat, sekä mahdollisuudet liikkuvaan työntekoon. Nykyaikana etätöiden tekeminen on saanut lisäsuosiota. Tästä johtuen kirjautuminen palveluihin pitää myös turvata entistä paremmin. Kirjautumista turvaamaan kehitettiin two factor authentication. Tämä tarkoittaa kahden tunnistustavan menetelmää. Ennen älypuhelimien yleistymistä käytettiin autentikaattoreita, jotka olivat fyysisiä laitteita. Niistä luettiin koodi, joka syötettiin kirjautuessa palveluun. Nykyään autentikaattorit ovat muuttuneet digitaalisiksi. Älypuhelimiin on saatavilla autentikaattoreita ohjelmisto muodossa. Autentikaattorit toimivat yleensä siten, että palveluun kirjauduttaessa palvelu pyytää autentikaattori koodia, luetaan sen antama koodi ja syötetään se palveluun.

Käyttäessä vähintään kahden tunnistustavan menetelmä on kirjautuminen vahva. Vahva tunnistautuminen voidaan myös hoitaa esimerkiksi salasanan ja sähköpostiin lähetyn koodin syöttämisellä. Tällöin tiedetään että kirjautuja on todellakin se kuka hän väittää olevansa. Multifator autentikointi lisää kahden tunnistustavan menetelmään vielä ainakin yhden tunnistustavan. Niitä ovat esimerkiksi, kirjautujan maantieteellinen paikka IP-osoitteen perusteella, sormenjälki tai vaikka henkilökortti. Lisää tietoa multifactor autentikoinnista tietoturvan yhteydessä.

Nykyajan liikesuuntaus tietojenkäsittelyn alalla on hajauttaminen sekä liikkuvuus. Pilvipalvelut tukevat hyvin liikkuvuuden tavoittelua ja ovatkin siksi olleet kovassa nosteessa. Käyttäjähallinto liittyy hyvin läheisesti tietojenkäsittelyn ja pilvipalveluiden maailmaan. Vielä vähän aikaa sitten kaikki palvelut vaativat omat

käyttäjätunnukset. Tästä johtuen käyttäjillä saattoi olla liikaa tunnuksia muistettavaksi. Tunnuksia saattoi olla kymmeniä ja kaikkiin piti olla omat ja erilaiset käyttäjänimi ja salasana parit. Pahimmillaan käyttäjät kirjoittivat tunnuksensa ylös paperille, jonka hukkuessa piti kaikkiin palveluihin vaihtaa tunnukset. Mikäli palvelut on ulkoistettu, voi pelkästään salasanojen vaihtamisesta syntyä huomattava lasku yritykselle. Espoon kaupungilla on hyvä esimerkki hinnoittelusta. Yksi salasanan vaihto maksaa kaupungille 18 euroa. Varsinkin kesälomilla työntekijät unohtavat herkästi työasiat, näihin kuuluvat salasanat. ”Voi olla, että neljän viikon kesäloman jälkeen en muista enää salasanaani. Se on ainakin merkki siitä, että loma on ollut rentouttava ja työasiat ovat unohtuneet” (Björksten, 2014). Tästä kertyykin vuodessa huomattava summa. Espoon kaupunki maksoikin vuonna 2014 salasanojen vaihtamisesta 200 000 euroa. Maksu voidaan sopia sopimusta tehdessä sisällytettäväksi kuukausittaiseen maksuun, mutta se ei kuitenkaan ole kovin halpaa (Björksten, 2014). Nykyään suuntaus tuntuukin olevan yhden kirjautumisen suuntaan. Tämä helpottaa käyttäjien taakkaa muistaa useita eri tunnusyhdistelmiä.

Tunnuksien käyttö on kuitenkin tärkeää, vaikka niistä onkin jonkin verran vaivaa. Tunnukset kertovat palvelulle kuka käyttää palvelua. Käyttäjällä voi olla monia tunnuksia, mutta tunnuksilla vain yksi käyttäjä. Kun tiedetään käyttäjätunnus, pitäisi silloin käyttäjänkin olla selvillä. Käyttäjähallinnan kautta voidaan määrittää mitä tietoja tai palveluja tunnuksella voi käyttää. Käyttäjätunnus voi olla vaikka asiakkaan nimi. On kaksi eri tapaa jakaa tunnuksia asiakkaalle. Joko annetaan asiakkaan itse päättää tunnus. Tällöin käyttäjätunnukset saattavat ottaa mitä mielikuvituksellisimpia muotoja, jolloin niiden hallinnoiminen saattaa hankaloitua. Toinen tapa on määrittää käyttäjätunnus itse asiakkaille. Tähän tapaan käytetään yleensä automaatiota. Yleisimmät kaksi tapaa, joilla automaatio toteutetaan, joko muodostaa ja yhdistelee käyttäjän etu- ja sukunimistä tunnuksen tai poimii sähköpostiosoitteen, jota käytetään tunnuksena.

Käyttäjähallinnossa määritellään jokaiselle käyttäjälle hänelle kuuluvat käyttöoikeudet. Näiden käyttöoikeuksien määrittely onkin tärkeää tehdä oikein. Mikäli käyttöoikeuksien määrittelyssä tehdään virheitä, voivat väärät käyttäjät päästä käsiksi sellaisiin tietoihin, joihin heitä ei pitäisi päästää. Kuvittele tilanne, jossa kuka tahansa käyttäjä pääsisi lukemaan kaikkien toisten käyttäjien sähköposteja. Tällainen

tilanne olisi, ei pelkästään tietosuojalain vastainen, vaan myös kiusallinen ja epäkäytännöllinen. Kuvittele, jos kenelläkään ei olisi henkilökohtaista sähköpostia, vaan kaikki sähköpostit olisivat yhdessä isossa kansiossa kaikkien luettavissa, ja sähköposteja lähetetään joidenkin lähteiden mukaan noin 205 miljardia kappaletta päivässä.

2 PILVIPALVELUT

Teoksessaan ”Pilvipalvelut” Petteri Heino kertoo mistä termi cloud computing eli pilvipalvelut tulee. Hänen mukaansa nimitys tulee tavasta dokumentoida puhelin ja tietoliikenneverkkoja. Koska verkot ovat monimutkaisia ja niissä on paljon yksittäisiä laitteita, kuvan piirtäminen verkoista vaikeutuu. Verkon esittämisen yksinkertaistamisuuden vuoksi ne on esitetty pilvisymbolilla. Tästä on peräisin nimitys ”pilvi” (Heino, 2010, 9).

Arkikielessä puhuttaessa pilvipalveluilla tarkoitetaan yleensä verkkotallennustilaa, kuten Microsoftin OneDrive tai Dropbox. Nämä palvelut ovatkin kuluttajille tutuimpia mutta, eivät suinkaan ainoita. Erilaisia pilvipalveluita löytyy paljon. Kuluttajille tuttuja pilvipalveluita ovat myös esimerkiksi useat sähköpostipalvelut. Sähköpostipalveluita ei yleensä mielletä pilvipalveluiksi. Hyvänä esimerkkinä Googlen gmail. Sähköpostisi on saatavilla mistä tahansa internetiin yhdistetystä laitteesta. Sinun ei tarvitse mennä samalle laitteelle, jolla olet Gmail-tilisi luonut, lukeaksesi sähköpostejasi.

Monelle pienemmälle yritykselle olisi liian kallista ostaa omia fyysisiä laitteita, kun on mahdollista ostaa palvelin, tai palveluiden käyttöoikeuksia palveluna. Tällä tavalla hankitun palvelimen tai palvelun etuna on yleensä hyvä muokkautuvuus ja alkuinvestoinnin pienuus. Palveluiden saatavuus ja helppo käyttöönotto saattaa olla jopa haitaksi.

Mikäli työntekijä hankkii itselleen henkilökohtaista tallennustilaa, voi hän helposti viedä arvokkaitakin tietoja yrityksen ulkopuolelle tahallisesti tai tahattomasti.

Tahattomasti tietojen vuotaminen yrityksen ulkopuolelle voi tapahtua käyttämällä epäluotettavaa palveluntarjoajaa tai salaamatonta yhteyttä tallentaessa tietoja palvelimelle. Samoja ongelmia liittyy esimerkiksi sähköpostin käyttämisessä salaamattomana, turvattoman yhteyden kautta tai käyttäjän kirjautuessa palveluun varomattomasti, paljastaen kirjautumistietonsa ulkopuolisille katsojille. Tietoturva asioita käsitellään lisää myöhemmin.

2.1 Pilvipalveluiden esittely

Pilvipalvelut ovat siis internetistä hankittua laskentakapasiteettia, palvelusuoritteita tai sovelluksia. Pilvipalvelut voidaan esittää niinkin, että se on toimintamalli, jonka kautta voidaan luopua fyysisistä konesaleista. ”Se on paljon kiinnostavampi debatin aihe kuin akateeminen keskustelu pilvipalvelun tunnistamisesta” (Heino 2010, 32). Pilvipalvelulla tarkoitetaan siis kaikkia tietoliikenneyhteyden yli käytettäviä palveluita.

Hyvä esimerkki palveluista on suosiotaan alati kasvattaneet verkkotallennustilat (Esim. Dropbox, Google Drive ja OneDrive). Käyttäjän on mahdollista ottaa käyttöön henkilökohtainen verkkotallennustila ja kasvattaa sitä tarpeen mukaan kuukausimaksulla. Sähköposti palvelut toimivat samalla periaatteella. Ne ovat yleensä yksityiskäyttäjälle ilmaisia palveluita. Yrityksille löytyy maksullisia palveluita, joita ostamalla saadaan esimerkiksi oman yrityksen nimellä oleva sähköpostiosoite ja yleensä parempi tai nopeampi asiakaspalvelu. Samantapainen järjestelmä on myös ostettaessa palvelimia tai laskentatehoa. Näitä palveluja silti harvemmin käyttävät yksityiskäyttäjät, mutta sekin on mahdollista.

Pilvitoimijoiden palvelut ovat myös suositumpia kuin koskaan aikaisemmin. Facebookin käyttäjämäärä oli kesäkuussa 2015 lähellä 1,5 miljardin aktiivista kuukausittaista käyttäjää. ”Yhtiön mukaan sillä oli kesäkuussa 1,49 miljardia aktiivista kuukausittaista käyttäjää, joista 1,39 miljardia kytkeytyy Facebookiin mobiililaitteiden kautta. Päivittäisiä aktiivikäyttäjiä on 968 miljoonaa ja näistä 844 miljoonalla on mobiiliyhteys. Päivittäisten aktiivikäyttäjien kokonaismäärä on kasvanut vuodessa 17 prosentilla. Vastaava kasvuluku pelkästään mobiilikäyttäjien

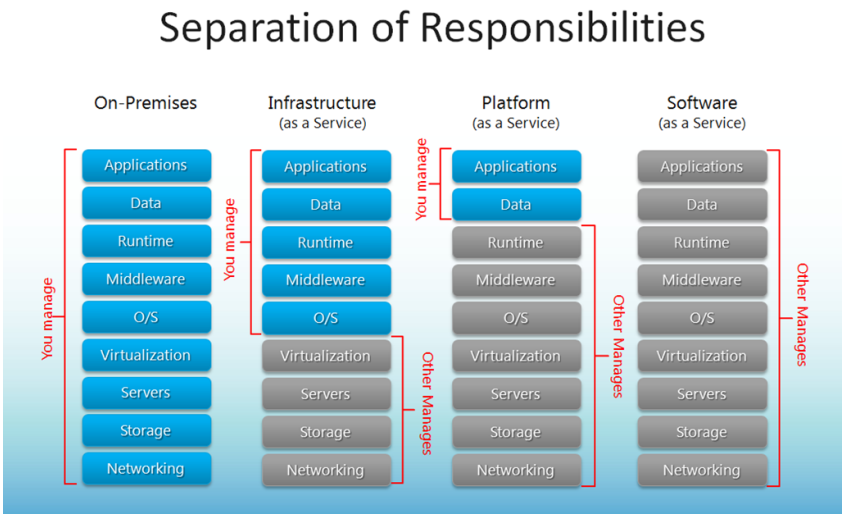
kohdalla oli 29 prosenttia” (Öhrnberg, 2015). Näistä luvuista voidaan todeta, ettei ainakaan Facebookin palveluiden käyttö ole laskussa. Facebook tarjoaakin erinomaisen pilvipalvelun. Sitä on myös alettu hyödyntää käyttäjähallinnan merkeissä. Siitä lisää myöhemmin.

Vanhempia ja suositumpia palveluja ovat esimerkiksi sähköpostit. Monet käyttäjät eivät välttämättä miellä sähköpostia pilvipalveluksi, mutta ne toimivat kuitenkin saman liikkuvuuden suovilla tavoilla. Käyttäjä kirjautuu palveluun mistä tahansa internetiin liitelyltä laitteelta, jolloin hänellä on käytössä samat tiedot kaikkialla.

Pilvipalveluja tuottavaa tahoa kutsutaan pilvipalveluntarjoajaksi tai pilvitoimijaksi. Nämä kaksi kannattaa eriyttää toisistaan. Pilvipalveluntarjoaja, joko yritys tai yhteisö, jonka kanssa on sopimus etukäteen määritellystä palvelusuoritteesta. Lisäksi on myös Pilvitoimijoita; sellainen on esimerkiksi Facebook. Sen palveluita käytetään, mutta sen kanssa ei ole tehty sopimusta käytetyn kapasiteetin mukaisesta laskutuksesta.

2.2 Pilvipalveluiden luokittelu

“Pilvipalveluita on kolmea perustyyppiä: Platform as a Service, Infrastructure as a Service ja Software as a Service” (Heino 2010, 50). Pilvipalvelut on luokiteltu muutamaan päätyyppiin teknisen toteutustavan perusteella. Toteutustapa kertoo, minkälaisia tietojenkäsittelytehtäviä pilvipalvelusta saadaan ja miten kyseessä olevaan koneistoon liitytään ja miten sen hallinnointi jakaantuu (kuva 1).

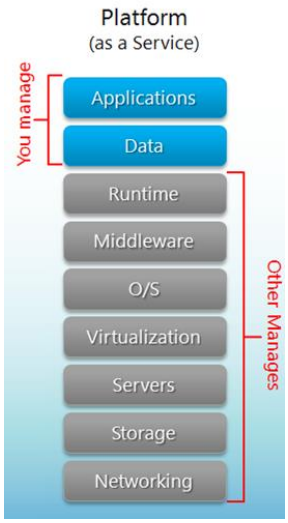


Kuva 1 Pilvipalveluissa vastuun jako asiakkaan ja palveluntarjoajan välillä. (Business insider www-sivut)

IT-alan tapa kuvata palvelua tai kapasiteettia kerroksilla ei sovellu kovinkaan hyvin kuvaamaan näitä palveluja. Esitystapa ja kuvaamisen perusidea on usein samankaltainen kuin OSI-mallissa. Pilvipalveluissa pyritään samaan viiden kerroksen pinona (client, application, platform, infrastructure, server). Asiakas voi ottaa käyttöönsä pilvipalveluita vain siltä kerrokselta kuin tarvitsee. Hänen ei tarvitse toteuttaa muita pinoja saadakseen mallin hyödyt käyttöönsä. Tämän takia pino ei ole kovin hyvä pilvipalveluiden esitystapa (Heino 2010, 50).

2.2.1 Platform as a Service (PaaS)

Platform as a Service- eli PaaS-tyyppisessä pilvipalvelussa koneiston tarjoajalla on täysin virtuaalinen palvelin ympäristö. Asiakkaan tarpeen mukaan palvelun tarjoaja jakaa asiakkailleen palveluita. Asiakkaat käyttävät palveluita API-ohjelmointirajapinnan (application programming interface) kautta. Asiakas teettää itse haluamansa sovellukset palvelimelle (Heino 2010, 51). Kuva 2 kuvaa miten vastuu hallinnasta jakaantuu käyttäjän ja palveluntarjoajan välillä.

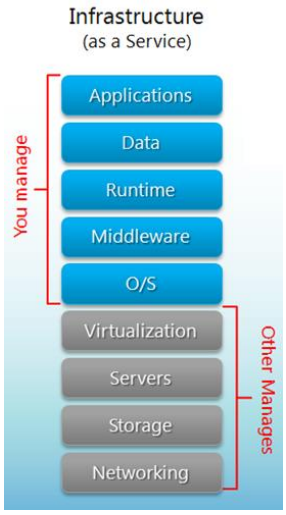


Kuva 2 Platform as a Service-palvelussa vastuun jako asiakkaan ja palveluntarjoajan välillä. (Business insider www-sivut).

Tätä mallia hyödyntävät parhaiten sellaiset asiakkaat, jotka pystyvät itse tuottamaan omat sovelluksensa. ”PaaS-koneiston käyttäminen tuotantosovellusten ajamiseen ei onnistu lennossa. Asiakkaalta tarvitaan jonkin verran viitseliäisyyttä, jotta ympäristö saadaan pystyyn ja sinne syntyy tarpeelliset ylläpitorutiinit” (Heino 2010, 51).

2.2.2 Infrastructure as a Service (IaaS)

IaaS-tyyppisessä pilvipalvelussa tarjoaja ylläpitää internetissä virtuaalista konesalia tai konesaleja. Niistä palvelun tarjoaja lohkoo asiakkaille etukäteen määriteltyjä ja hinnoiteltuja osioita ja antaa ne asiakkaan käyttöön. Asiakas voi perustaa näihin lohkoihinsa tarvitsemansa käyttöjärjestelmät ja sen päälle sovelluksensa (Heino 2010, 52). Kuva 3 selittää IaaS palveluissa asiakkaan ja palveluntarjoajan hallinnoinnin vastuunjakoa.

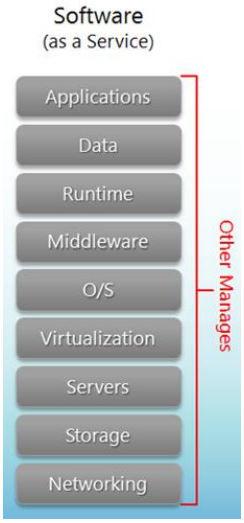


Kuva 3 Infrastructure as a Service-palvelussa vastuun jako asiakkaan ja palveluntarjoajan välillä. (Business insider www-sivut).

”Tässäkin tapauksessa asiakkaalta vaaditaan osaamista ja kärsivällisyyttä käynnistämisessä ja ylläpidollisissa rutiineissa, mutta tekniikka ja tavat ovat tuttuja, jos omassa käytössä on ollut virtuaalisoinnin isäntäkoneita” (Heino 2010, 53).

2.2.3 Software as a Service (SaaS)

Software as a Service tarkoittaa nimensä mukaisesti sovelluksen hankkimista pilvipalveluna. Sovellus jaetaan tietoliikenneyhteyden kautta käyttäjille. Palveluntarjoaja huolehtii kaikesta muusta (Heino 2010, 53). Kuvassa 4 näkyy, miten SaaS palveluissa palveluntarjoaja hoitaa kaiken hallinnoinnin.



Kuva 4 Software as a Service-palvelussa vastuun jako asiakkaan ja palveluntarjoajan välillä. (Business insider www-sivut)

Palveluntarjoaja käyttää elastisen provisioinnin, virtualisoinnin ja jaetun ympäristön tapoja, joten sovellusten tarvitseman kapasiteetin tuotantokustannus on edullisempi kuin se, mihin asiakas itse pääsisi. (Heino 2010, 54)

2.3 Pilvi tyypit

Pilvipalvelut voidaan jaotella sen mukaan miten palvelu tuotetaan. Palvelu voidaan tuottaa, joko yrityksen oman verkon sisältä, jolloin palvelun nimenä on private cloud. Palvelu voidaan ostaa yrityksen ulkopuolelta julkisesta verkosta, jolloin palvelun nimenä on public cloud. Voidaan toteuttaa näiden kahden palvelutyypin yhdistelmänä, jolloin puhutaan hybrid cloudista.

2.3.1 Public cloud

Public cloud on nimensä mukaisesti julkinen palvelu. Palveluntarjoaja tarjoaa palveluinaan esimerkiksi sovelluksia ja tallennustilaa julkisesti internetin välityksellä. Julkisen pilven palvelut voivat olla ilmaisia, tai niistä voidaan periä maksu sopimuksen mukaan. (Techtarget.com 2013)

Public cloud -palvelun tarjoaja tuottaa palveluita yleisesti asiakkaiden käyttöön internetin välityksellä. Tietylle asiakkaalle ei siis ole varattu tiettyjä fyysisiä resursseja palveluntarjoajan konesalissa. Asiakkaille lohkotaan sopimuksen mukaan resursseja.
”Public cloud on usein järjestetty siten, että asiakas saa kapasiteettia jaetusta ympäristöstä ilman omaa dedikoitua laitteistoa tai kapasiteettia, joskaan tämä ei ole public cloudin edellytys eikä sitä rajaava seikka” (Heino 2010, 54).

Palvelut voivat olla ilmaisia, tai palveluntarjoaja voi periä käyttäjältä maksun kuukausi-, tunti- tai muun aikaan sidotun veloituksen. Palveluntarjoaja voi myös laskuttaa käytetyn kapasiteetin mukaan.

2.3.2 Private cloud

Private cloud toimii kuten muutkin pilvipalvelut, mutta se tuotetaan yrityksen oman verkon sisällä. Täten saadaan turvallisuutta ja muuntautuvuutta. Tässä mallissa asiakas järjestää ja omistaa itse pilvipalvelukoneistonsa. Asiakas myös huolehtii ylläpitoprosesseista itse (Heino 2010, 55)

”Parhaimmillaan private cloud–malli mahdollistaa tehokkaan it-resurssien käytön ja siten paremman hyötysuhteen investoinneille. Private cloudin ajatellaan tarjoavan parempaa palvelua it-toiminnolta käyttäjille muun muassa uusien palveluiden nopeamman käyttöönoton myötä” (Heino 2010, 55)

Private Cloud toteutus pyrkii välttämään monet pilvipalveluihin liitetyt turvallisuutta koskevat ongelmat. Koska private cloud toteutetaan oman yrityksen sisältä, sitä suojaa yrityksen oma palomuuri. Näin saadaan parempi tietosuoja datalle, koska data ei välttämättä poistu yrityksen tiloista. (Webopedia.com)

2.3.3 Hybrid cloud

Hybrid cloud on kahden edellisen tekniikan yhdistelmä. Siinä pilvipalvelu toteutetaan oman verkon sisällä ja se yhdistetään ulkopuolisen palveluntarjoajan

palveluun. Yritys voi säästää tarvitsemiansa resursseja jakamalla kriittiset datat ja käsittelyt oman verkkonsa sisällä pyörivään pilvipalveluun ja ajaa ei niin kriittiset ajot tai datasäilöt kolmannen osapuolen ylläpitämiin palveluihin.

Yritys voisi käyttää oman verkkonsa sisältä tuotettua palvelua kaikkiin ajoihin, mutta mikäli palvelussa ajetaan paljon dataa, voi järjestelmä hidastella tai kaatuilla. Siksi saattaakin olla järkevää jakaa kriittiset ja ei niin kriittiset tarpeet eri palveluihin. Kriittiset ajot on järkevää hoitaa oman verkon sisällä, jotta tietoliikenneongelmat ja datan kaappaaminen eivät tuota ongelmia. Palvelun työkuormaa voidaan helpottaa viemällä osa tai kaikki ei niin kriittisestä ajosta oman verkon ulkopuolelle. Ei niin kriittisiä ajoja ovat esimerkiksi testaus ja kehitys ajot. Private cloudin ja public cloudin yhdistäminen onnistuu tähän tarkoitetulla ohjelmistolla (Techtaget 2015).

2.4 Pilvitoimijat

Pilvitoimija eroaa pilvipalvelusta siinä, että pilvipalvelun kanssa tehdään sopimus, jossa määritellään palvelu ja siitä maksettava käyttömaksu. Käyttömaksu perustuu käytettyjen resurssien suuruuteen. Pilvitoimijan kanssa ei tehdä erikseen sopimusta käytetyistä resursseista ja niistä maksamisesta. Pilvitoimijoita ovat esimerkiksi Google ja Facebook.

Pilvitoimijan kanssa tehdään käyttäjäsopimus, mutta sen palveluiden käyttö on yleensä maksutonta. Esimerkkeinä Facebook ja Google, joiden palveluiden käyttö on loppukäyttäjälle ilmaista. Profiilin luominen Facebookiin on ilmaista ja Googlen hakupalvelut ovat ilmaisia. Tulonsa pilvitoimija saa mainostuksesta. Mainostamisessa käytetään kohdennettua mainontaa. Molemmat esimerkkeinä toimineista toimijoista keräävät käyttäjistään tietoja, joiden avulla mainoksia kohdennetaan käyttäjien hakujen tai profiilin tietojen mukaan.

2.4.1 Google

Suurin yksittäinen pilvitoimija on kiistämättä Google. Sen tarjoamia palveluja, perinteisen hakukoneen lisäksi, ovat esimerkiksi Gmail, Youtube ja Google+. Näiden palveluiden lisäksi Google tarjoaa huomattavan määrän palveluita. Mainittavaa on myös esimerkiksi Googlen mainoskoneisto AdSense ja AdWords. Nämä mainoskoneistot pyörivät isossa osassa internetiä. Mainosten tuottavuus onkin Googlelle hyvä rahasampo. Vuonna 2006 Google ilmoitti tuloikseen 10492 miljardia dollaria mainostuksesta ja vain 112 miljoonaa muita tuloja. Vuonna 2011, 96% Googlen tuloista olikin peräisin mainoskoneistosta (Wikipedia www-sivut).

Pilvitoimijat eivät saa tuloja suoraan loppukäyttäjiltä, toisin kuin pilvipalvelun tarjoajat. Pilvitoimijat saavat tulonsa suurimmaksi osaksi mainostuksesta. Facebookin kautta mainostaminen ei joidenkin raporttien mukaan ole yhtä kannattavaa kuin Googlen kautta. Googlen mainoksissa käyttäjä klikkaa mainokseen noin 8 % varmuudella, kun taas Facebookissa vastaava prosentti on vain 0.04 (Bloomberg 2007). Iso osa Facebookin mainospuhetta onkin, että sillä on niin paljon tietoa käyttäjistänsä, että se pystyy kohdentamaan mainoksiansa todella tehokkaasti. “Jos Facebook pystyy todistamaan väitteensä, sen ei tarvitse huolehtia niin paljoa kilpailijoistaan” (Matthews 2014). Google on lanseerannut Facebookkia vastaavan palvelun Google+, mutta sitä ei ole otettu vastaan yhtä innokkaasti kuin Facebookkia. Tästä huolimatta Google on tuonut kirjautumispalveluita yritysten käyttöön.

Google Sign-In on Googlen tuottama autentikointipalvelu. Tämän autentikoimispalvelun kautta voidaan käyttäjille antaa mahdollisuudet käyttää Googlen palveluita, esimerkiksi Google Drivea tai Google+. Yritys voi siis tarjota oman palvelunsa lisänä Googlen palveluita. Google tarjoaa yrityksille, jotka haluavat käyttää sen autentikoimispalveluita, niiden käyttöönottoa helpottavan Identity Toolkit paketin. (Googlen www-sivut)

Pakettia käyttämällä yritys voi helposti ottaa käyttöönsä isompien autentikointipalveluiden tarjoajien palvelut. Näihin palveluntarjoajiin kuuluvat esimerkiksi Google ja Facebook. Paketti tarjoaa yritykselle helpon tavan ottaa autentikoimispalvelu käyttöön. Tämä paketti tarjoaa myös Smart Lock for

Passwords, Single Sign-on palvelun. Sen avulla käyttäjät autentikoidaan Android-mobiililaitteilla käytettäviin sovelluksiin ja Chrome selaimella käytettäviin sivustoihin Automaattisesti, käyttäjän niin halutessa.

2.4.2 Facebook

Facebook antaa käyttäjilleen mahdollisuuden luoda oma käyttäjäprofiilin ja sen kautta luoda itselleen ystävä-verkoston. Profiilin kautta käyttäjä voi liittyä itseään kiinnostaviin ryhmiin ja siten luoda itselleen kustomoitu uutissyöte etusivulleen. Mainokset kustomoidaan käyttäjän profiilin mukaan ja niin käyttäjälle pyritään tuomaan häntä kiinnostavia mainoksia (Facebook www-sivut). Varsinkin nuoremmat käyttäjät ovat kuitenkin hyviä lukemaan internetiä ja siten pystyvät halutessaan paremmin välttämään mainoksia (Gawker www-sivut). Yrityksille on myös mahdollista luoda oma käyttäjäprofiili palveluun.

Oman käyttäjäprofiilin kautta yritykset pyrkivät mainostamaan omia tuotteitaan ja tuomaan uutisia seuraajilleen. Profiilin kautta hoidetaan markkinointia, uutisointia ja asiakaspalvelua. Yritykselläkin profiilin luominen on ilmaista, mutta mainostaminen maksaa erikseen. Yrityksen mainokset näytetään käyttäjille, jotka ovat profiiliensa mukaan kiinnostuneita aiheesta. Facebookkia on alettu käyttämään myös käyttäjien autentikoimispalveluna (Facebook www-sivut).

Yritykset ovat alkaneet tarjota mahdollisuutta kirjautua omaan palveluunsa käyttäjän Facebook profiilin kautta. Mikäli käyttäjällä on Facebook tili, voi hän kirjautua toiseen palveluun ilman erillistä rekisteröitymistä. Facebook autentikoi käyttäjän oman palvelunsa kautta, linkittäen käyttäjän palveluun. Kun käytetään Facebook kirjautumista, Facebook toimittaa tietoja palveluun, johon kirjaudutaan. Näihin tietoihin kuuluu esimerkiksi käyttäjän nimi, sähköpostiosoite, sukupuoli ja käyttäjän tykkäykset. Käyttämällä Facebookin palvelua voidaan saada käyttäjästä paljon tarkempi kuva kuin ehkä olisi mahdollista saada tietoja itse keräämällä. Palveluita, jotka tarjoavat Facebook kirjautumis mahdollisuuden, on jo paljon erilaisia ja niitä kehitetään kokoajan lisää (Facebook www-sivut).

2.5 Kehityssuunta

Nykyaikana yritykset ’syntyvät pilveen’. Tämä tarkoittaa sitä, että kun uusi yritys pystytetään, ei ole järkeä ostaa kalliita fyysisiä palvelinlaitteistoja, kun on mahdollista ostaa ne palveluina yrityksen ulkopuolelta. Ostettaessa iso osa yrityksen tarpeista palveluina ulkopuolelta, ei vaadita niin isoja rahallisia alkupanostuksia yritykseen kuin ennen on vaadittu.

Tämä helpottaa yrityksen perustamista huomattavasti. Monessa tapauksessa juuri alkunsa saaneet yritykset pystyvät ostamaan avaimet käteen-tyyppisiä palveluita. Tällöin yrityksen rahallinen ja työmäärällinen panos jää minimaaliseksi. Yrityksen ei ole tarpeellista heti alkutaipaleellaan panostaa suureen IT-tuki osastoon. Yritys pääsee heti hyödyntämään palveluiden tuomista eduista, ilman liian suuria panostuksia. Kun yritys on päässyt tukevasti jaloilleen, voidaan palveluita toteuttaa yrityksen sisältä, jolloin palveluiden kustannukset eivät enää ole liian kalliita nuorelle yritykselle.

Tämä malli on nurinkurinen entisaikaan nähden. Ennen yritykset ovat joutuneet toteuttamaan tarvittavat palvelut itse, jolloin kynnys aloittaa uusi yritys on ollut huomattavasti korkeammalla kuin nykyään.

2.6 Palvelun osto tai itse tuottaminen

Yrityksen tilanne määrittelee hyvin pitkälle kannattaako pilvipalvelu ostaa yrityksen ulkopuolelta vai tuottaa itse. Rahallisesti mitattuna saattaa olla halvempaa ostaa palvelu yrityksen ulkopuolelta. Palveluita voidaan räätälöidä hyvinkin tarkasti yrityksen tarkoituksiin sopivaksi. Tällöin hinta voidaan neuvotella sopivaksi. Mikäli kuitenkin yritys haluaa tuoda kriittisempiä tietoja tai palveluita pilveen, saattaa olla tietoturva mielessä turvallisempaa tuottaa palvelu itse.

Palvelun tuotto yrityksen sisällä on yleensä ainakin alkukustannuksiltaan kalliimpaa kuin sen ostaminen ulkopuoliselta palveluntarjoajalta. Palvelun aloittamiseen pitää hankkia fyysistä laitteistoa. Yleisesti ottaen palvelimen pystyttäminen yrityskäyttöön

on kallista. Kuitenkin säästöä saattaa syntyä pitkällä tähtäimellä, jos hankinnat tehdään viisaasti.

Hyvin suunniteltu palvelu tuo yritykselle lisäarvoa kun taas huonosti suunniteltu voi käydä kalliiksi. Mikäli yritys päättää itse tuottaa pilvipalvelun, tarvitaan siihen fyysiset palvelin laitteistot. Laitteistojen hankinnassa pitää laskea laitteiston elinkaari ja aika kauanko laitteilla tuotettavaa palvelua tarvitaan.

Kustannuksia tuovat fyysisten laitteiston lisäksi osaaminen. Palvelinten saattaminen käyttökelpoisiksi on monen työtunnin takana. Tähän tarvitaan osaavaa työvoimaa. Työvoimaa tarvitaan myös palvelinten ylläpitämiseksi. Yrityksen kannalta saattaa olla edullisempaa ostaa palvelut ulkopuoliselta palveluntarjoajalta, mikäli sillä ei ole valmiina asiantuntevaa IT-osastoa. Osaavan henkilöstön palkkaaminen pelkästään yhtä toimintoa varten ei yleensä ole hyvin kannattavaa.

Palvelua ostaessa parhaassa tapauksessa voidaan saada avaimet käteen tyyppinen palvelu, joka tarkoittaa ettei palvelun käyttäjän tarvitse itse tehdä palvelulle mitään.

3 KÄYTTÄJÄHALLINTA

Ennen AD:n (Active Directory) kehittämistä tietokoneiden käyttö yrityksissä tai yhteisöissä tarkoitti jokaiselle käyttäjälle oman tietokoneen hankintaa ja sitä että tiedostot, joita käyttäjä omalla tietokoneellaan loi, oli käytettävä vain kyseisellä tietokoneella. AD:n kehitys muutti yrityksissä ja yhteisöissä tietokoneiden yhteiskäyttöä vapaampaan suuntaan. Ennen jokaisella käyttäjällä oli henkilökohtaiset tietokoneet, joille muut eivät voineet kirjautua tietämättä tietokoneen salasanaa. AD:n yleistyessä voitiin yrityksille ja yhteisöille hankkia tietokoneita yhteiseen käyttöön.

AD mahdollisti työtekijän kirjautumisen mille tahansa koneelle omilla tunnuksillaan, mahdollistaen täten omien tiedostojensa ja jaettujen resurssien käyttämisen miltä tahansa verkkoon yhdistetyltä koneelta. Nykyisellä tietojenkäsittelyn aikakaudella

arvostetaan liikkuvuutta ja sopeutuvuutta. Active Directory ei kuitenkaan rajoitu pelkästään käyttäjien tietoihin.

AD:sta löytyvät käyttäjien lisäksi verkkoon liitetyt resurssit. Resursseja ovat esimerkiksi tulostimet, tietokoneet ja reitittimet. Kaikkia näitä laitteita pitää myös hallita, siihen Active Directory soveltuu erittäin hyvin. Järjestelmän hallinnoija pystyy AD:n kautta helposti ja tehokkaasti hallinnoimaan ryhmäpolitiikkaa ja käyttöoikeuksia. Hallinnointi helpottuu huomattavasti käytettäessä ryhmäpolitiikkaa.

Mikäli ryhmäpolitiikkaa ei käytetä, pitää jokaisen käyttäjän kohdalla erikseen määritellä oikeudet. Tämän tekeminen manuaalisesti veisi paljon aikaa, varsinkin isommissa organisaatioissa. Ryhmäpolitiikalla voidaan kerralla määrittää monen käyttäjän tai laitteen ominaisuuksia.

Hakemiston pitäisi olla enemmän kuin pelkästään tehokas tapa löytää tietoa. Hakemistossa pitäisi myös pystyä hallitsemaan tietoa. Jos meillä on liikaa paikkoja joista haemme tietoa, voimme saada ristiriitaisia tai vanhentuneita tietoja, joiden läpikäyminen voi olla aivan yhtä turhauttavaa, kuin päämäärätön selailu. On tärkeää, että tietty tieto saadaan yhdestä lähteestä. Silloin meidän ei tarvitse etsiä tietoa monesta eri paikasta. (Arkills, 2003, 4).

3.1 Directory as a Service (DaaS)

DaaS, eli Directory as a Service on moderni, pilvessä toimiva käyttöjärjestelmästä ja laitteistosta riippumaton hakemistopalvelu. Sen avulla voidaan hallinnoida IT resursseja, laitteen tyypistä tai sen käyttöjärjestelmästä riippumatta. (Jump Cloud 2016). Hakemiston toimiessa pilvipalveluna, siihen voidaan päästä käsiksi milloin ja mistä vain.

Modernin hakemiston pitää siirtyä pilvipohjaiseksi palveluksi, joka pystyy autentikoimaan, valtuuttamaan ja hallinnoimaan käyttäjiä, laitteita ja ohjelmistoja. Tämän pitäisi tapahtua mahdollisimman pienellä panostuksella IT-tuen puolelta

(Rajat 2014). Hakemisto palveluna tuo IT-tuelle helpotusta. Erinäisten hakemistojen yhdistelmät ovat vaikeasti hallittavissa. Uuden palvelun myötä, eri hakemistot on helppo yhdistää ja täten helpottaa käyttöä, niin käyttäjälle kuin IT-tuelle.

3.2 Active Directory

Active Directory eli, AD, on Microsoftin Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. Se mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja sovelluksille sekä tarjoaa tavan nimetä, paikallistaa, hallita, suojata ja kuvata käytössä olevia verkon resursseja. Hakemisto mahdollistaa käyttäjien liikkuvuuden verkossa olevien tietokoneiden välillä. AD:n myötävaikutuksella voit siis kirjautua mille tahansa verkkoon liitetylle koneelle, tehdä tarvittavat toimenpiteet ja käyttää tarvittavia resursseja. AD:n oli kehittänyt Microsoft käytettäväksi Windows toimialueella. Ensimmäisen kerran Active Directory julkaistiin Windows 2000 Serverille ja sitä paranneltiin seuraavissa Windows Server julkaisuissa. Tämän jälkeen Active Directoryn toimintoja ja hallinnointi ominaisuuksia laajennettiin Windows Server 2003 versiossa. Uusien Windows Server versioiden mukana julkaistiin paranneltuja versioita AD:sta. Windows Server 2008:ssa julkaistiin muiden uusien palveluiden ohella Active Directory Federation Service. Ennen käyttöjärjestelmän ydinominaisuus, joka hoiti domainien hallinnointia, nimettiin Active Directory Domain Serviceksi (ADDS). Siitä tuli keskeinen palvelinrooli. (Wikipedia, Active Directory 2016).

Active Directory on laajentunut huomattavasti sen julkaisusta Windows 2000 Serverillä. Jos Active Directoryä käytettiin aluksi vain keskitettyyn domainien hallintaan, on se nykyisin paljon enemmän. Nykyään suurin osa kaikista hakemisto pohjaisista palveluista ovat AD:n alla. Sieltä löytyvät esimerkiksi verkkoon kytketyt käyttäjät, tulostimet, tietokoneet ja reitittimet (Clines, Steve, Loughry, Marcia. 2008, 8).

Käyttämällä AD:ta ylläpito voidaan tehdä huomattavasti helpommin. Tiedot, joita tarvitaan etäkonfiguroimiseen, löytyvät AD:sta. Ilman ryhmäpoliikkaa jokaisen

laitteen ja käyttäjän käyttöoikeuksien ja muiden konfiguraatioiden tekeminen veisi tuhottomasti aikaa. Asettamalla tietyt laitteet ja tietyt käyttäjät oikeisiin ryhmiin, voidaan niiden huoltotoimenpiteet hoitaa nopeasti ja tehokkaasti. Esimerkkinä yhtiössä on vaikka sata työntekijää, jotka jaetaan vaikka myyntiin, huoltoon, johtoon ja tukeen. Jos jokaisen työntekijän kohdalla jonkun pitäisi manuaalisesti tehdä hänelle käyttäjätunnus ja määrittää mitä resursseja käyttäjä pääsee käyttämään yrityksen verkossa, menisi tähän toimitukseen liikaa aikaa ja resursseja. Vaihtoehtoisesti hallinnoija voisi määrittää ryhmät, joiden nimet olkoon myynti, huolto, johto ja tuki. Tämän jälkeen hänen pitää vain määrittää ryhmien käyttöoikeudet ja määrittää käyttäjälle ryhmä. Hallinnoijan käyttämä aika putoaa huomattavasti ja resursseja vapautuu muuhun käyttöön.

Hyvin määritellyt ryhmät nopeuttavat uusien työntekijöiden pääsemistä töihin. Aina uuden työntekijän hankkimisen myötä täytyy hänet liittää työpaikan verkkoon. Jos uuden työntekijän liittäminen yrityksen verkkoon viivästyy, ei hänestä ole hyötyä. Työntekijän liittäminen on siis hyvä olla mahdollisimman tehokas toimenpide, jolloin AD ja sen tarjoama käyttäjähallinta ryhmineen on huomattava apu.

Kun työntekijä, syystä tai toisesta, poistuu yrityksen palveluksesta, pitää hänen pääsynsä yrityksen järjestelmiin estää mahdollisimman nopeasti ja tehokkaasti. Työntekijä saattaa luoda yritykselle turvallisuusriskin. Mikäli poistuneella työntekijällä on pääsy yrityksen dataan, voi hän tehdä monenlaista haittaa yritykselle. Työtekijän poistuessa oikea-aikaisuus on siis avaintekijä. Mikäli pääsy tietoihin katkaistaan liian aikaisin, voidaan menettää viimeinen työpanos. Mikäli pääsy katkaistyaan liian myöhään, voi työntekijä tehdä haittaa yritykselle. Active directoryssa on kuitenkin yksi huomattava puute. Se ei tue Applen tuotteita, tabletteja tai Linux palvelimia. Tähän ongelmaan on kuitenkin tuotettu ratkaisu.

3.3 Jump Cloud

Jump Cloud on pilvipalveluna toimiva vaihtoehto Microsoftin AD:lle. Jump Cloud tukee kaikkia niitä resursseja, joita AD ei tue. Jump Cloud aloitti elämänsä startup projektina, jota johti Rajat Bhargava. Alun perin startup projekti pyrki tuomaan

markkinoille palvelimen hallinnointityökalua, mutta pian he tajusivat heillä olevan käsissään vaihtoehto AD:lle. (Dix 2015)

Jump Cloud yhdistää kaikki nykyaikaiset laitteet hakemistoon. Hakemisto toimii pilvipalveluna, joten se on käytettävissä mistä tahansa, milloin tahansa, kunhan vain tietoliikenneyhteys on käytettävissä. Jump Cloud on pohjimmiltaan palvelinten hallinta työkalu. Sillä voidaan hallita palvelimia ja käyttäjiä. Jump Cloud on myös helppo ottaa käyttöön, vaikka yrityksellä olisikin jo käytössä vanhempia käyttäjähallinta toteutuksia.

Jump Cloud voidaan yhdistää melkeinpä mihin tahansa vanhempaan toteutukseen, joka yrityksellä on jo käytössä. Näihin vanhempiin toteutuksiin kuuluvat esimerkiksi Microsoftin AD ja LDAP. Jump Cloud käyttää omaa tietokanta toteutusta, johon on kehitetty muille protokollille käyttörajapinnat. Mikäli tietokanta perustuu jonkin tiettyyn protokollaan, se saattaa helposti sulkea joitakin toisia protokollia käyttökelvottomiksi. Jump Cloudin toimitusjohtaja kertoi haastattelussa heidän päätyneen luomaan oma protokollansa ja luomaan siihen käyttörajapinnat muille tarvittaville protokollille. (Dix 2015).

Monien eri käyttörajapintojensa vuoksi Jump Cloud on helppo tuoda jo olemassa olevaan ympäristöön. Nykyaikana ympäristöön todennäköisesti kuuluu muitakin laitteita kuin pelkästään Microsoftin käyttöjärjestelmällä toimivia. Näitä ovat esimerkiksi Macit, Iphonet ja Unix-käyttöjärjestelmällä toimivat laitteet. Näiden laitteiden tukemattomuus on ollut ongelmallista AD:n dominomassa järjestelmässä. Pelkän AD:n avulla näitä laitteita ei pysty hallinnoimaan, jolloin ne olivat pahimmassa tapauksessa turvallisuus riski. Vähintäänkin laitteet jäivät paitsi verkkoresursseista ja IT tuesta. Nykyään Jump Cloudin ansiosta päästään näitäkin laitteita hallinnoimaan.

3.4 Microsoft Azure AD

Microsoft toi markkinoille uuden pilvipalveluita hyödyntävän hakemistojen ja henkilöllisyyksien hallinnointipalvelun nimeltään Azure Active Directory. Azure AD

on Microsoftin pilvipalveluna toimiva hakemisto-, ja käyttäjähallintapalvelu. Palvelu tarjoaa mahdollisuuden Single Sign-on kirjautumisen tarjoamiseen useisiin eri palveluihin. Näihin palveluihin lukeutuvat esimerkiksi Office365 ja Dropbox. (Vilcinskas, 2016).

Azure mahdollistaa yrityksille yhden kirjautumisen käytännön tarjoamisen työntekijöilleen. Yhden kirjautumisen käytäntö tarkoittaa ettei työntekijän tarvitse kirjautua jokaiseen työpäivän aikana käyttämäänsä palveluun erikseen. Tämä helpottaa salasanojen muistamista ja poistaa turhaa kirjautumisiin ja salasanojen muistelemisiin käytettyä aikaa. Yhden kirjautumisen käytäntöä selitetään lisää myöhemmin.

Azure AD sisältää laajan kapasiteetin identiteetinhallintaan. Näihin kuuluvat moninkertainen autentikointi, laitteiden rekisteröinti, omatoiminen salasanan- ja ryhmänhallinta. Azure AD voidaan integroida valmiiksi käytössä olevaan Windows serverin Active Directoryyn. Azureen vaihtavat yritykset voivat tehdä muutoksen helposti. (Vilcinskas, 2016).

3.5 LDAP

LDAP, eli Lightweight Directory Access Protocol on protokolla, jota useat ohjelmat (esimerkiksi e-mail ohjelmat) käyttävät löytääkseen tietoja tietokannoista. Tiedot eivät rajoitu vain henkilötietoihin tai e-mail osoitteisiin, vaan tietoja voi olla myös esimerkiksi salausavaimista ja verkossa olevista tulostimista. Protokolla kehitettiin Michiganin yliopistossa sopeuttaakseen monimutkaisen X.500 hakemistojärjestelmän nykyaikaiseen internetiin. X.500 on liian monimutkainen, jotta sitä voitaisiin käyttää internetin ylitse. LDAP kehitettiin, jotta palvelu saataisiin laajempaan käyttöön. (Gracion Software www-sivut)

LDAP palvelimia on kolmenlaisia. Isoja julkisia-, isoja yritysten käyttämiä palvelimia ja pienempiä palvelimia työryhmille. Suurin osa isoista julkisista palvelimista ovat kadonneet, koska ihmiset eivät halua julkaista omia sähköpostiosoitteitaan roskapostin takia. (Gracion Software www-sivut)

Jokaisessa sähköpostiohjelmassa on henkilökohtainen osoitekirja, mutta miten voidaan hakea sellaisen ihmisen sähköpostiosoite, joka ei koskaan ole lähettänyt sinulle sähköpostia? Miten yritys voi ylläpitää keskitettyä ja ajantasaista osoitekirjaa, johon kaikilla on oikeudet? Nämä kysymykset saivat yritykset, kuten Microsoft ja IBM, tukemaan LDAP-standardia. Protokollana LDAP ei määrittele miten ohjelmat toimivat. Se määrittelee kielen, jolla asiakasohjelmat ’puhuvat’ palvelimen kanssa tai palvelimet ’puhuvat’ keskenään. Suomeksi LDAP pyyntö voisi kuulostaa vaikka tältä: ”Hae ihmisistä kaikki, jotka asuvat porissa, joiden nimi sisältää ’Kalle’, joilla on sähköpostiosoite. Palauta koko nimi, sähköpostiosoite” (Gracion Software www-sivut).

4 PILVIPALVELUIDEN TUOMAT HAASTEET

Pilvipalveluiden, kuten minkään muunkaan tietotekniikan, käyttäminen ei ole aivan riskitöntä. Palveluiden hallitsematon käyttöönotto saattaa luoda riskin kriittisten tietojen vuotamiseen yrityksen ulkopuolelle. Pilvipalveluiden yleistyessä ihmisillä saattaa olla omia pilvitallennustilojaan, joille helposti ladataan työtietoja. Työntekijöiden aikeet voivat olla hyvät, jotkut heistä saattavat esimerkiksi haluta viimeistellä töitä omalla ajallaan. Tämä voi kuitenkin saattaa tiedot vaaraan joutua vääriin käsiin. Yrityksen IT-osaston on vaikea puuttua tietoturva asioihin työntekijöiden kotona. Tietoturva asioihin liittyy myös palveluntarjoajan omat tietosuojamäärittelyt. Mikäli käytät ulkopuolista datasäilöä, on data silloin jonkun muun huolen aihe. Jättäisitkö itse vaikka pankkitunnuksesi kaverillesi tai jollekin muulle yritykselle huolehdittavaksi?

Palveluntarjoajat antavat tietosuojalausunnon, jossa he määrittelevät miten tietoja säilytetään palvelussa. Mikäli asiakas hyväksyy lausunnon, hän voi käyttää palvelua. Tietosuoja on kuitenkin lopulta vain asiakkaan vastuulla. Yrityksen pitää päättää luottaako se ulkopuoliseen palveluntarjoajaan, ettei se vuoda tietoja muualle. Hyvinä esimerkkeinä työn kirjoittamisen aikaan vellovat keskustelut ja oikeustaistelut tietourkintaa koskevissa jutuissa. Mikäli lukijaa kiinnostavat keskustelut, niitä löytyy

hakemalla internetistä vaikka ’NSA ja tietosuoja’ hakusanoilla hakien. Vaihtoehtona on luoda yrityksen oma pilvipalvelu. Ulkopuolisilta palveluntarjoajilta voidaan helposti ostaa tarvittavat palvelut, jotta voidaan testata palvelujen tarvetta tai sopivuutta yritykselle. Luomalla omat palvelut, voidaan ehkä dataa hallita paremmin ja tiedetään, ettei data ole ulkopuolisten tahojen hoidettavana. Pilvipalveluiden hyödyllisyyttä voi olla vaikea mitata.

Mikäli palvelu ei suoranaisesti tuota rahaa yritykselle, palvelusta maksaminen voidaan nähdä tuhlauksena. IT-osaston saattaa olla vaikea tuoda esille miksi palvelu kannattaisi ottaa käyttöön ja miksi siitä kannattaisi maksaa. Se saattaa olla vaikeasti selitettävä konsepti asiasta tietämättömälle johdolle. Mahdollisia argumentteja palveluiden maksamisesta voisivat olla vaikka henkilöstötietojen hallittavuuden helpottaminen tai liikkuvuuden parantaminen.

5 PILVIPALVELUIDEN TURVALLISUUS

2010-luvun elämässä käyttäjillä on muistettavanaan monien eri palveluiden käyttäjänimiä ja salasanoja. Käyttäjät saattavatkin yrittää helpottaa muistettavien käyttäjänimi/salasana yhdistelmien määrää käyttämällä useissa palveluissa samoja yhdistelmiä. Tietoturvan kannalta tämä käytäntö ei ole kovinkaan suotavaa. Yrityksen menetykset voivat olla huomattavat, mikäli työntekijä on käyttänyt samoja yhdistelmiä monissa yrityksen arkaluontoisissa, kirjautumista vaativissa, tietokannoissa tai palveluissa. Toisaalta, yrityksen kannalta on myös kallista jos työntekijältä menee liikaa työaikaa kirjautua tarvitsemiinsa palveluihin. Tähän ongelmaan apuna voi toimia single sign-on ratkaisut. Single sign-on ratkaisee käyttäjän tarpeen muistaa monia erilaisia salasanoja ja helpottaa täten pääsyä tarvittaviin tietoihin.

Toisaalta yhden kirjautumisen ongelmana on sen helppokäyttöisyys. Mikäli ulkopuolinen taho pääsee käsiksi tarvittaviin kirjautumistietoihin, voidaan helposti päästä käsiksi kriittisiin tietoihin. Tietoturva on jatkuvaa nuoralla tanssimista. Mikäli pääsyä helpotetaan liikaa, on helposti vaarana tietojen vuotaminen ulkopuolisille.

Mikäli tietoturvasta tehdään liian tiukkaa, saattaa työtekijöiden työpanos kärsiä. Liikkuvuuden aikakaudella etätyöskentely on helpompaa ja suositumpaa kuin aikaisemmin.

Pilvipalvelut mahdollistavat ennen näkemättömän liikkuvuuden työntekijöille. Koska työpaikan palveluihin on mahdollista päästä käsiksi vaikkei työntekijä fyysisesti työpaikalla olisikaan, tuo se uusia mahdollisuuksia niin hyvään kuin huonoonkin käytökseen. Yritys voi hyötyä, mikäli työntekijät voivat tehdä töitään ympäri vuorokauden ja mistä tahansa paikasta, jossa on internet yhteys. Tämä kuitenkin tuo myös uusia ongelmia turvallisuuden kanssa.

Mikäli työntekijä käyttää salaamattomia yhteyksiä, kirjautuu näkyvästi yrityksen palveluihin tai hänen työvälineenään toimiva kannettava tietokone varastetaan saattavat yrityksen tiedot olla vaarassa. Turvallisuuden näkökannasta riskitekijöitä pitäisi karsia, mutta se ei aina ole helppoa. Yrityksen IT-tuki voi järjestää koulutustilaisuuksia, joissa kerrotaan vaaratekijöistä.

5.1 Tietoturva

Pilvipalveluiden tietoturvan ongelmat liittyvät lähinnä siihen, että kun tiedot ovat netissä, ovat ne periaatteessa kaikkien saatavilla. Mikäli tiedot ovat yrityksen omalla palvelimella, johon ei ole pääsyä yrityksen verkon ulkopuolelta. Ovat tiedot suhteellisen turvassa. Mikäli tietoja halutaan kaapata, pitää päästä fyysisesti palvelimen lähelle. Mikäli yritys kuitenkin haluaa tuoda tiedot saataville palveluun internetin yli, on tehtävä riskianalyysi.

Analyysissä tulee punnita palvelun käyttöönotosta aiheutuvia haittoja ja mahdollisia hyötyjä. Yleisimpiä hyötyjä ovat todennäköisimmin työntekijöiden liikkuvuuden paraneminen, työntekijöiden etätyömahdollisuudet paranevat ja tietoja on helpompi jakaa yrityksen sisällä. Yrityksen pitää kuitenkin punnita tietojen helppokäyttöisyyden ja tietoturvan heikkenemisen välillä. Yleisimpiä haittoja ovat tietojen vuotaminen yrityksen ulkopuolelle ja tietojen saatavuus ongelmat. Jos tiedot ovat helpommin saatavilla työntekijöille, saattaa se myös helpottaa

tietoturvavuotojen sattumista. Yrityksen pitää myös ottaa huomioon tietoliikennekatkojen mahdollisuus. Mikäli jostakin syystä tietoliikenne takkuilee, voi tietojen käyttäminen olla hitaampaa tai mahdotonta. Tästä syystä kaikkein kriittisimpiä tietoja ei välttämättä pitäisikään säilyttää yleisessä verkossa. Kun kuitenkin päätetään käyttää pilvipalveluja, pitää käyttäjät autentikoida.

Tämän hetken turvallisin autentikointimetodi on multifactor autentikointi. Multifactor autentikointi toimii useammalla kuin kahdella autentikointi menetelmällä. Kirjaudut siis palveluihin jollakin mitä sinä tiedät (käyttäjätunnus ja salasana) ja jollakin hallussasi olevalla välineellä (esimerkiksi puhelimella, sähköpostilla tai henkilökortilla). Hallussasi oleviin välineisiin kuuluvat esimerkiksi autentikaattorit (digitaaliset tai fyysiset), geopaikannus, sormenjäljet, henkilökortit, matkapuhelimet ja paljon muita. Näitä autentikointi metodeja yhdistelemällä saadaan eri tilanteissa toimivia autentikointi tapoja. Monipuolisten yhdistelmien tuoman turvan ja muokattavuutensa takia multifactor authentication onkin tämän hetken turvallisin autentikointimetodi. Esimerkiksi kirjautuminen palveluun kaksivaiheisen kirjautumisen käyttöönoton jälkeen. Ensin käyttäjä syöttää palveluun Sen mitä se tietää, eli käyttäjätunnuksen ja salasanan. Tämän jälkeen häneltä kysytään esimerkiksi matkapuhelimeen tekstiviestinä lähetetty koodi. Kirjautumisen jälkeen käyttäjä voi valita, ettei häneltä enää kysytä puhelimeen lähetettyä koodia, mikäli käyttäjä kirjautuu samalta laitteelta. Kun hän kirjautuu seuraavan kerran palveluun samalta laitteelta palvelu varmistaa laitteen olevan sama kuin ensimmäisellä kerralla. Palvelu luottaa käyttäjätunnuksen ja paikallistamisen avulla, että käyttäjä on sama kuin edelliselläkin kerralla. Ensimmäisessä tapauksessa käyttäjältä pyydetään käyttäjätunnusten jälkeen todistamaan hänellä olevan hallussaan jokin laite, tässä tapauksessa matkapuhelin. Kun nämä kaksi asiaa on todennettu, käyttäjä autentikoidaan palveluun. Toisessa autentikointi tapahtuu käyttäjätunnuksien ja laitteen tunnistamisen avulla (Google inc. www-sivut).

5.2 Tietosuoja

Palveluntarjoajat tarjoavat tietosuojalausunnon, jossa kerrotaan palveluntarjoajan tietosuojamenettelyt. Tietosuojalausunnosta ilmenee muun muassa miten tietoja

käsitellään, säilytetään ja pidetäänkö tiedot salassa, vai käytetäänkö niitä johonkin, esimerkiksi markkinointiin. Kaikkien palveluita käyttävien, kannattaisi olla tietoisia palveluntarjoajan tietosuojalausunnosta. Yrityksille tämä on ehdottoman tärkeä dokumentti, joka pitäisi käsitellä, kun tehdään päätöksiä palveluista. Lausunnon avulla voidaan punnita mahdollisia hyötyjä ja haittoja.

Vaikka palveluntarjoaja kertoo lausunnossa, miten tietoja käsitellään, pitää asiakkaan silti olla varovainen siitä, mitä tietoja palvelussa käsitellään. Vaikka palveluntarjoaja antaisikin takuun siitä, että tiedot säilytetään salassa, on kuitenkin lopullinen vastuu mahdollisessa tietovuoto tapauksessa asiakkaalla. Näitä ongelmia voidaan kuitenkin minimoida.

Kaikista turvallisin pilvipalvelu tietosuoja näkökannasta on yrityksen oma pilvipalvelu. Yrityksen oma pilvipalvelu tarkoittaa palvelua, jonka yritys tuottaa itse. Se hankkii tarvittavat laitteistot, jolloin tiedetään datan fyysinen sijainti. Tällöin ei ole vaaraa että ulkopuolinen palveluntarjoaja pääsisi dataan käsiksi.

5.3 Single sign-on

Single sign-on (SSO) tarkoittaa kertakirjautumista moniin kirjautumista vaativiin palveluihin. Palvelu toteutetaan yleensä LDAP protokollan ja palvelinten yhteistyöllä. Kertakirjautumisella tarkoitetaan yhden käyttäjänimi/salasana yhdistelmän syöttämistä ja sisäänkirjautumista moneen palveluun samanaikaisesti. Kirjautumisen jälkeen ei siis tarvitse enää kirjautua uudestaan moneen eri palveluun.

Palvelusta löytyy myös käänteisversio, Single sign-off. Tämä tarkoittaa monesta palvelusta uloskirjautumista samaan aikaan. Tämä palvelu olisi hyvä sisällyttää palveluihin, jotka käyttävät SSO:ta. Mikäli käyttäjä kirjautuu vain kertaalleen moneen eri palveluun, ei hän välttämättä tajua että hänen pitäisi myös kirjautua ulos monesta eri palvelusta. Tämä unohdus saattaisi mahdollistaa tunkeutumisen palveluihin, joista käyttäjä on unohtanut kirjautua ulos. Käyttäjä ei välttämättä tiedä mihin kaikkiin palveluihin hän on SSO:ta käyttämällä kirjautunut. Nämä palvelut yhdessä tuovat helpotusta käyttäjien kirjautumistietojen muistamiseen. Palvelu auttaa

myös IT-tuen ajankäyttöön poistamalla turhia kirjautumistietojen kyselyitä ja niiden uudelleenasettamisia. Single Sign-off palvelut ovat kuitenkin vaikeampia toteuttaa. Palvelua on kritisoitu siitä, että se saattaa helpottaa pääsyä liikaa. Mikäli käyttäjän kirjautumistunnukset vuotavat ulkopuolisen käyttöön, voidaan päästä liian syvälle yrityksen kriittisiin tietokantoihin, ilman että tiedetään varmaksi, kuka tietoihin on päässyt käsiksi.

Tähän ongelmaan avuksi tuodaankin vahvat autentikointimetodit. Näistä henkilökohtaisesti parhaaksi koen sirulliset henkilökortit. Mikäli käyttäjille annetaan sirulliset kortit, kirjautumiset tapahtuvat syöttämällä kortti lukijaan, jonka jälkeen käyttäjä antaa salasanansa. Korteissa on kuitenkin se heikkous että käyttäjä voi helposti unohtaa korttinsa jonnekin, mistä sen voi ulkopuolinen taho saada haltuunsa. Pelkän kortin menettäminen ei kuitenkaan tarkoita vielä tietoturvan murtumista, koska kortin pariksi tarvitaan salasana tai pin-numero. Käyttäjän huoleksi jääkin salasanan tai numeron muistaminen. On kuitenkin mahdollista että käyttäjä kirjoittaa hankalasti muistettavan numeron paperille, jolloin se voi joutua ulkopuolisten käsiin.

Nykyaikana suosittuja palveluita voidaan myös käyttää autentikoimaan käyttäjiä toisiin palveluihin. Esimerkkinä Facebook, jonka kautta voidaan kirjautua moneen erilaiseen palveluun. Esimerkiksi Spotify-palveluun voidaan kirjautua facebookin kautta. Kun käyttäjä avaa Spotify-ohjelman, häneltä kysytään käyttäjätunnusta ja salasanaa. Vaihtoehtona tarjotaan Facebook-kirjautuminen. Jos käyttäjä valitsee Facebook-kirjautumisen, hänet viedään Facebookin kirjautumissivulle. Siellä käyttäjä kirjautuu Facebook tunnuksillaan palveluun, jolloin Facebook lähettää Spotify ohjelmaan autentikointi tiedon, josta ilmenee, kuka käyttäjä on. Tämän jälkeen käyttäjä pääsee käyttämään Spotifyn palveluita.

6 YHTEENVETO

Pilvipalveluilla tarkoitetaan siis internetissä toimivaa palvelua, joita yritykset ja yksityiset henkilöt voivat ostaa kuukausihintaisena palveluna. Palveluihin hyvinä esimerkkeinä kuuluvat verkkotallennustilat ja sähköpostipalvelut.

Palveluita tarjoavia tahoja kutsutaan joko pilvipalveluntarjoajiksi tai pilvitoimijoiksi. Erona näillä on palvelusuhteen määrittelyssä. Palveluntarjoajan kanssa on tehty etukäteen sopimus, jossa määritellään palvelusuorite. Näihin kuuluu esimerkiksi Dropbox. Dropbox tarjoaa pilvitallennustilaa etukäteen määritellyn palvelusopimuksen mukaan. Pilvitoimijat ovat yrityksiä, jotka toimivat pilvessä ja joiden kanssa ei ole tehty sopimuksia datankäyttömaksuista. Esimerkkinä toimii Facebook. Facebook toimii pilvessä, mutta käyttäjät eivät ole tehneet sopimuksia palvelun kapasiteetin käytöstä. Pilvipalvelut on luokiteltu erilaisiin palvelutyyppeihin.

Luokitukset ovat; public, private ja hybrid cloud. Public, eli julkinen pilvi tarkoittaa palvelun tuottamista suurelle yleisölle. Palvelun resursseja jaetaan käyttäjien sopimuksien mukaisesti. Yhdelle käyttäjälle ei ole varattu tiettyä fyysistä laitetta, vaan kaikki käyttäjät jakavat resurssit. Private, eli yksityinen pilvi tarkoittaa yrityksen sisältä tuotettua palvelua, jossa resurssit on tarkoitettu vain tietylle asiakkaalle. Hybrid, eli yhdistelmä pilvi. Yhdistelmä pilvi on nimensä mukaisesti yhdistelmä yksityisestä ja julkisesta palvelusta.

Palveluita voidaan joko ostaa yrityksen ulkopuolelta, tai tuottaa itse. Varsinkin pienet ja uudet yritykset hyötyvät palveluista, koska ne eivät vaadi suurta alkupääomaa. Palvelut on mahdollista ostaa yrityksen ulkopuolelta ja mahdollisuuksien mukaan siirtyä julkisesta palvelusta itse tuotettuun yksityiseen palveluun. Monet uudet yritykset syntyvätkin nykyään pilveen. Yleensä on paljon halvempaa ostaa tarvittavat palvelut alussa yrityksen ulkopuolelta. Näin toimiessa voidaan panostaa johonkin muuhun tarvittavaan, eikä tarvitse itse hankkia kallista rautaa.

Käyttäjähallinta on ollut suuressa roolissa tietokoneiden yleistyessä yrityksissä. Käyttäjähallinnan kehittymisen myötä on tullut mahdolliseksi ottaa yrityksissä käyttöön jaettuja resursseja. Näihin resursseihin kuuluvat muun muassa tietokoneet ja tulostimet. Käyttäjähallinnan myötä voidaan luoda eri henkilöille omat käyttäjätunnukset. Tunnuksien myötä pystytään käyttäjille jakamaan resurssit ja asettamaan rajoitukset. Kaikkien käyttäjien ei tarvitse saada samoja resursseja käyttöönsä, pystyä käyttämään samoja ohjelmia tai päästä käsiksi kaikkiin

tiedostoihin. Active Directory, eli AD onkin ollut suuressa roolissa käyttäjähallinnan kehityksessä. AD:n myötä voitiin jakaa käyttäjät ryhmiin. Käyttäjien oikeuksia on helpompi hallita, kun ne jaetaan ryhmiin. Kun ryhmien käyttöoikeudet määritellään oikein, ei uusien työntekijöiden tullessa yritykseen, tarvitse kuin luoda käyttäjätunnus ja lisätä hänet oikeisiin ryhmiin. Mikäli ei käytetä ryhmittelyä, pitää jokaiselle käyttäjälle manuaalisesti määritellä käyttöoikeudet. AD:n oikea käyttö voikin säästää yrityksen hallinnointikustannuksissa huomattavasti aikaa ja siten myös rahaa. AD ei kuitenkaan ratkaise kaikkia nykyajan käyttäjähallinnan ongelmia. Suurin ongelma AD:ssa on, ettei se tue nykyistä laitteiston ja käyttöjärjestelmien laajuutta.

AD ei tue Applen tuotteita, tabletteja eikä älypuhelimia. Nämä laitteet ovat aikaisemmin jääneet käyttäjähallinnon ulkopuolelle. Tähän ongelmaan on nyt ratkaisu, Jump Cloud. Se tuo kaikki sellaiset laitteet käyttäjähallinnan piiriin, mitkä AD jätti ulkopuolelle. Jump Cloud on toteutettu sitä varten luodulla tietokantaprotokollalla, johon on luotu käyttörajapinnat muille protokollille. Tämän takia Jump Cloud on helppo tuoda yrityksen jo mahdollisesti olemassa olevaan ympäristöön. Kun laitteet, joita ennen Jump Cloudia ei ole saatu käyttäjähallinnan alaisuuteen, päästään niitä hallinnoimaan. Kun laitteita hallinnoidaan oikein se tuo lisää tietoturvaa yritykseen. Voidaankin siis todeta että käyttäjähallinto liittyy myös läheisesti yrityksen tietoturvaan (Dix, 2015).

Työntekijän poistuttua yrityksen palveluksesta tai hänen tehtäviensä muuttuessa on tärkeää saada nopeasti tehtyä muutoksia hänen käyttöoikeuksiinsa. On tietoturvariski jos käyttäjällä on pääsy yrityksen tietoihin tämän lähdettyä yrityksen palveluksesta. Tietoturva on jatkuvaa tasapainottelua käytettävyyden ja turvallisuuden välillä. Mikäli tietoturva on liian löysää, voi sattua tietomurtoja. Mikäli tietoturva on liian tiukkaa, voi työaikaa mennä hukkaan, kun työntekijät eivät pääse käsiksi tarvittaviin tietoihin. Single sign-on palvelut ovat omiaan helpottamaan pääsyä tietoihin.

Single sign-on tarkoittaa kertakirjautumista useaan palveluun samalla kerralla. Tämä helpottaa pääsyä, mikäli työntekijän pitää kirjautua moneen eri palveluun. Palvelu helpottaa käytettävyyttä huomattavasti, mutta kirjautumiseen olisi suositeltavaa käyttää vahvaa tunnistautumista, jotta tiedetään kuka tietoja käyttää. Google ja

Facebook ovat alkaneet tarjota autentikoimis palveluita. Niiden hyvinä puolina yrityksille on niiden käyttöönoton helppous ja niiden tuomat lisäpalvelut. Googlen kirjautumispalveluita käyttämällä voidaan tarjota Googlen muita palveluita yrityksen sovelluksen tai palvelun sisällä. Otetaan esimerkkinä yritys joka tuottaa uutissyötettä. Palveluun Googlen kirjautumispalvelulla kirjautunut asiakas voi esimerkiksi jakaa uutissyötteitä Google+ palveluun. Mikäli taas käytettäisiin Facebookin autentikoimispalvelua, voisi asiakas jakaa uutissyötteitä Facebookiin. Lisänä autentikoimispalveluiden käyttämisen hyviin puoliin pitää laskea Googlen ja Facebookin käyttäjien tuntemus. Koska Facebook ja Google ovat molemmat pitkään keränneet käyttäjistään tietoja, niiden tietojen käyttäminen helpottaa yrityksen omaa toimintaa huomattavasti. On paljon helpompaa käyttää valmiina olevaa tietokantaa, kuin luoda itse uusi.

Pilvipalveluiden hyödyntäminen todennäköisesti lisää etätyö mahdollisuuksia ja niiden haluttavuutta ja toimivuutta. Etätöissä on kuitenkin omat hyvät ja huonot puolensa. Toisaalta etätyöskentely antaa työntekijöille suuremman vapauden tehdä töitä silloin ja siellä kun he haluavat. Toisaalta se saattaa myös lisätä paineita olla tavoitettavissa tai töissä myös vapaa-ajallaan. Yritysten ja työntekijöiden onkin löydettävä sopiva tasapaino työn ja vapaa-ajan välillä alati kehittyvässä maailmassa.

Uusia palveluita tuodaan jatkuvasti markkinoille. Nämä palvelut kehittyvät jatkuvasti ja kiihtyvään tahtiin. Mikäli suuntaus jatkuu samanlaisena kuin teoksen kirjoittamisen aikaan, jonka uskonkin jatkuvan, tulemme näkemään yhä kasvavan palveluiden kirjon. Nykymaailmassa olemme tottuneet siihen että meidän on mahdollista saada melkeinpä kuka tahansa ihminen kiinni lähes mihin tahansa aikaan päivästä tai vuodesta.

Tulevaisuudessa en näe että hylkäämme mobiililaitteitamme ja siitä syystä pilvipalveluiden tulevaisuus näyttääkin todella hyvältä. Alan kasvu tuottaa varmasti työpaikkoja niin uusien palveluiden visioimisessa, kuin vanhojen palveluiden ylläpidossa. Uskon myös etätyöskentelyn kasvuun. Etätyöskentely on varmasti yksi pilvipalveluiden parhaimpia mahdollisuuksia ja käyttäjähallinnon suurimpia haasteita.

LÄHTEET

Arkills, B. 2003. LDAP Directories Explained. Pearson Education, Inc

Björksten, T. 2014. Lomalla unohtuneista salasanoista tulee jättilasku työnantajalle – jopa 200 000 euroa vuodessa. Viitattu 16.05.2016. https://yle.fi/

Bloomberg www-sivut. 2007. Facebook May Revamp Beacon. Viitattu 15.05.2016. https://bloomberg.com/

Business insider www-sivut. 2013. Viitattu 18.05.2016. http://businessinsider.com/

Clines, Steve, Loughry, Marcia. 2008. Active Directory for dummies. For Dummies

Denton, N. 2007. Facebook 'consistently the worst performing site'. Viitattu 15.05.2016 https://Gawker.com

Dix, J. 2015. Directory-as-a-Service lets you extend Active Directory to all those items AD can't support. Viitattu 12.05.2016. https://Networkworld.com

Facebook www-sivut. Viitattu 18.05.2016. https://facebook.com/

Google Inc. www-sivut. Viitattu 18.05.2016. http://google.com

Gracion Software www-sivut. Viitattu 07.03.2016. http://www.gracion.com/

Heino, P. 2010. Pilvipalvelut. Hämeenlinna. Talentum Media Oy

Jump Cloudin www-sivut. Viitattu 11.05.2016. https://jumpcloud.com

Jump Cloud 2016. Jump Cloudin julkaisu. Viitattu 11.05.2016. http://go.jumpcloud.com/rs/jumpcloud/images/what-is-DaaS-directory-as-a-service.pdf

Matthews, C. 2014. More Than 11 Million Young People Have Fled Facebook Since 2011. Viitattu 15.05.2016. https://business.time.com/

Microsoftin www-sivut. Viitattu 14.02.2016. https://Microsoft.com/

Networkworld www-sivut. Viitattu 09.05.2016 https://Networkworld.com

Rajat Bhargava. 'What is a directory in the cloud era'. Jump Cloud blog. 24.09.2014. Viitattu 11.05.2016. https://jumpcloud.com/blog/what-is-a-user-directory-cloud-era/

Rosendahl C. 2014. The beginners guide to multi-factor authentication. SMS Passcode.

Techtarget www-sivut. Viitattu 13.02.2016. https://techtarget.com/

Webopedia www-sivut. Viitattu 13.02.2016. http://webopedia.com/

Wikipedian www-sivut. Viitattu 08.03.2016. https://en.wikipedia.org/

Wikipedian www-sivut. Viitattu 08.03.2016. https://fi.wikipedia.org/

Ylen www-sivut. Viitattu 16.05.2016. https://yle.fi/

Öhrnberg, P. 2015. Facebook ylitti odotukset - käyttäjämäärät vakaassa kasvussa. Viitattu 18.05.2016. http://kauppalehti.fi