TAMPEREEN
AMMATTIKORKEAKOULU

SALASANAPALVELUN IMPLEMENTOINTI TUOTANTOYMPÄRISTÖÖN

Olli Lehmussaari

Opinnäytetyö
Toukokuu 2018
Tietojenkäsittelyn
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkkopalvelut

LEHMUSSAARI, OLLI:
Salasanapalvelun implementointi tuotantoympäristöön

Opinnäytetyö 29 sivua
Toukokuu 2018

Tämä opinnäytetyö tehtiin pirkanmaalaiselle ICT-alan yritykselle. Toimeksiantajalla oli tarve asentaa heidän tuotantoympäristöönsä palvelu, jonka avulla käyttäjät voisivat nollata unohtuneen tai vanhentuneen salasanansa itse ilman teknisen tuen apua. Opinnäytetyön tavoitteena oli kehittää toimeksiantajan asiakaspalvelua, pienentää käyttäjän salasanan unohtumisesta tai vanhentumisesta syntyvää haittaa asiakasyritykselle ja toimeksiantajalle sekä parantaa toimeksiantajan salasananvaihtoprosessin tietoturvallisuutta. Tarkoituksena oli implementoida toimeksiantajan tuotantoympäristöön ennalta valittu salasanapalvelu, jonka avulla tavoitteet pystyttäisiin saavuttamaan. Opinnäytetyössä tutkittiin pilvipalveluiden käyttötarkoitusta ja palvelumalleja, sekä tietoturvallisuuden yleisiä tavoitteita ja käyttäjän todentamiseen liittyviä haasteita.

Lopputuloksena tuotantoympäristöön asennettiin palvelu, johon asiakasyritysten käyttäjät pääsevät yhdistämään nettiselaimella. Salasanaa nollatessa palvelu lähettää käyttäjälle ennalta määrättyyn puhelinnumeroon tekstiviestillä kertakäyttöisen salasanan, jonka avulla käyttäjän henkilöllisyys todennetaan. Tämän avulla käyttäjä pääsee nopeammin kirjautumaan takaisin pilvipalveluun ja näin ollen jatkamaan töitään. Työn toteutusta on kuvattu vain yleisellä tasolla, sillä toimeksiantaja katsoi, että yksityiskohtaiset tiedot tuotantoympäristöstä, esimerkiksi IP-osoiteavaruuksista, laskisivat sen tietoturvallisuutta.

Opinnäytetyö onnistui suunnitellusti ja salasanapalvelu ja siihen tarvittavat lisäpalvelut saatiin toimimaan halutunlaisesti. Salasanapalvelun käyttäjämäärien kasvaessa saamme varmasti palautetta palvelun käytöstä ja palvelua voidaan kehittää saadun käyttäjäpalautteen avulla.

Asiasanat: salasana, salasanapalvelu, implementointi, pilvipalvelut

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Network Services

LEHMUSSAARI, OLLI:
The Implementation of a Password Self-Service in a Production Network

Bachelor's thesis 29 pages
May 2018

This study was made for the Finnish IT-firm Magic Cloud Oy. The client provides cloud services for their customers and their services consist of, for example, virtual desktops. The client wanted to install a password self-service into their production network. With the service their users could reset their password in case it was forgotten or expired without the help of client's helpdesk. The goal was to improve the client's customer service and to reduce the loss of productive working hours due to forgotten or expired password. With the self-service installed, the users can log into the cloud service faster and the client's helpdesk can focus on more productive tasks than password reset. Another goal was to improve the security of the password reset process.

As the result of the study a password self-service was installed to the client's production network. Users can reset their password and the user authentication is done by one-time-password sent to the user's predefined phone number. The study's execution is described in general because the client view was that describing specific details of their production network weakens its security.

The study succeeded well and the password self-service and the necessary add-ons worked as was planned. In the future when the number of users increases we can collect feedback about the service and improve it.

Key words: password, self-service, implementation, cloud

SISÄLLYS

1 JOHDANTO

Tämä opinnäytetyö on tehty pilvipalveluja tarjoavalle pirkanmaalaiselle ICT-alan yritykselle, Magic Cloud Oy:lle. Toimeksiantaja on erikoistunut tarjoamaan erilaisia kirjanpidon ja palkanlaskennan ohjelmia pilvipalveluna ja tarjoaa lisäksi esimerkiksi pilvestä tallennuskapasiteettia. Toimeksiantajalla oli toiveena saada implementoitua tuotantoympäristöönsä salasanapalvelu, jonka avulla heidän asiakasyritysten käyttäjät pystyisivät vaihtamaan unohtuneen tai vanhentuneen salasanansa nopeasti, vaivattomasti, turvallisesti ja ilman toimeksiantajan teknisen tuen apua. Palvelun avulla käyttäjät pääsevät nopeammin kirjautumaan sisälle pilvipalveluun ja unohtuneen tai vanhentuneen salasanan vaihtaminen tapahtuu turvallisemmin, kun salasanapalvelun avulla käyttäjän puhelinnumeroon voidaan lähettää varmennusviesti.

Työn tavoitteena oli kehittää toimeksiantajan asiakaspalvelua, sekä parantaa pilvipalvelunsa tietoturvallisuutta. Lisäksi työn tavoitteena on parantaa sekä toimeksiantajan, että asiakasyritysten työn tuottavuutta, kun käyttäjät pääsevät nopeammin palaamaan töihinsä ja toimeksiantajan teknisen tuen henkilökunta voi paremmin keskittyä tuottavampiin töihin. Työn tarkoituksena oli asentaa toimeksiantajan tuotantoympäristöön salasanapalvelu, jonka avulla työn tavoitteisiin päästiin.

Opinnäytetyötä varten etsin lähdeaineistoa, jossa käsiteltiin pilvipalveluita, tietoturvaa, käyttäjän todentamista, salasanoja ja salasanakäytäntöjä. Etsityn lähdemateriaalin avulla tutustuin pilvipalveluiden käyttötarkoituksiin, tietoturvan pääkohtiin, käyttäjän todentamisen eri tapoihin ja salasanojen käytäntöihin ja niiden tärkeyteen palveluiden tietoturvan kannalta.

Opinnäytetyössä asennettava palvelu oli valittu jo ennen opinnäytetyöprosessin alkua erään kurssityön tuloksena. Opinnäytetyö rajattiin salasanapalvelun asentamisen suunnitteluun ja toteutukseen. Työssä käydään palvelun asennusprosessi läpi yleisellä tasolla, sillä toimeksiantajan tuotantoympäristön yksityiskohtaiset tiedot, kuten esimerkiksi IP-osoitteet ja domain nimet ovat tärkeitä ympäristön turvallisuuden kannalta.

2 PILVIPALVELUT

2.1 Pilvipalveluiden määritelmä

Pilvipalveluille ei ole olemassa yleisesti hyväksyttyä yksiselitteistä määritelmää. Internetistä käytetään usein kielikuvaa pilvi ja pilvipalveluilla tarkoitetaan mallia, jossa tietotekniikkaresursseja, kuten esimerkiksi dataliikenne, laskenta- ja tallennuskapasiteettia, tarjotaan verkon välityksellä. (Viestintävirasto 2014). Pilvipalveluiden ominaisuuksiin kuuluu, että käyttäjän ei tarvitse tietää missä resurssit sijaitsevat tai huolehtia niiden toiminnasta tai ylläpidosta. Yhdysvalloissa julkishallinnon standardeja pohtivan paikallisen elinkeinoministeriön alainen NIST (National Institute of Standards and Technology) on tehnyt seuraavanlaisen määritelmän pilvipalveluille ”Pilvipalvelut on toimintamalli, joka mahdollistaa pääsyn vapaasti konfiguroitaviin ja skaalautuviin tietotekniikkaresursseihin, jotka voidaan ottaa käyttöön tai poistaa käytöstä helposti ja nopeasti.” (Salo 2012, 16–17.)

NIST nimeää yleisen määritelmänsä lisäksi viisi pilvipalveluiden ominaispiirrettä. Näitä ovat itsepalvelullisuus, pääsy palveluihin eri päätelaitteilla, resurssien yhteiskäyttö, nopea joustavuus ja käytön tarkka mittaaminen (Salo 2012,17). Itsepalvelullisuudella tarkoitetaan, että pilvipalvelun käyttäjä saa tarvitessaan käyttöönsä tai ottaa pois käytöstään tietotekniikkaresursseja ilman, että hänen tarvitsee olla yhteydessä palveluntarjoajaan (Rouse & Moore 2016). Resurssit ovat siis juuri silloin saatavilla, kun niille on tarvetta, eivätkä aiheuta kuluja, jos niitä ei tarvita. Päätelaiteriippumattomuudella tarkoitetaan, että palveluiden käyttö on mahdollista niin työasemilla, kannettavilla tietokoneilla kuin mobiililaitteillakin. (Salo 2012, 17.)

Pilvipalvelun resurssien hyödyntäminen onnistuu parhaimmillaan pelkän verkkoyhteyden avulla. Resurssien yhteiskäytössä asiakkaan ei tarvitse tietää eikä hän yleensä ole oikeutettu saamaan tietoa siitä, kuinka ja missä hänen ostamansa pilvipalvelu toteutetaan. Yhdellä palveluntarjoajalla voi olla samanaikaisesti useita eri asiakkaita käyttämässä samaa laite- ja ohjelmistokapasiteettia toisistaan tietämättä tai riippumatta. Pilvipalvelut ovat usein hyvin skaalautuvia. Laitekapasiteettia voidaan lisätä asiakkaan palveluihin nopeasti, kun kyseisen asiakkaan palvelun käyttöaste on korkea. Vastaavasti kun käyttöaste laskee, voidaan laitekapasiteettia helposti pienentää,

jolloin asiakasta ei laskuteta ylimääräisestä käyttämättömästä kapasiteetista. Resurssien käyttö on tarkkaan mitattu ja valvottu pilvipalveluympäristöissä. Useissa palvelumalleissa laskutus tapahtuu käytettyjen resurssien mukaan ja tätä varten tarvitaan tarkkaa tietoa yksittäisen asiakkaan resurssien käytöstä. Tämän avulla asiakas voi luottaa laskutukseen ja pystyy myös seuraamaan omaa resurssien käyttöään. (Salo 2012, 17–18.)

Pilvipalvelun ei kuitenkaan tarvitse olla ulkoisen palveluntarjoajan tuottama palvelu, vaan myös yrityksen oma yllämainittuja ominaisuuksia noudattama toimintamalli voi olla pilvipalvelu. Tällaisessa tapauksessa palvelun tuottaa ja käyttää yritys itse. Tällöin kyseessä on yksityinen pilvi. Pilvipalveluiden hankintatapoja on neljä. (Viestintävirasto 2014). Yksityisen pilven vastakohta on julkinen pilvi. Tällä tarkoitetaan, että pilvipalvelu ostetaan ulkopuoliselta palveluntarjoajalta. Tällöin pilvipalvelun hallinnointi, laitteisto, ohjelmisto ja palvelut ovat palveluntarjoajan hallinnassa. Yhteisöllisen pilven pilvipalveluinfrastruktuuri voi olla useamman organisaation tai järjestön yhteiskäytössä ja -omistuksessa. Palvelun hallinnoinnista voi huolehtia ulkopuolinenkin taho ja infrastruktuuri voi sijaita jossain muualla kuin palvelun käyttäjien omissa tiloissa. Neljäntenä mallina on hybridipilvi. Tällöin kyseessä on edellä mainittujen palvelujen yhdistelmä. Osa pilviarkkitehtuurista on yksityistä tai yhteisöllistä ja osa julkista. (Salo 2012, 18.)

2.2 Pilvipalvelumallit

Teknisen toteutuksensa perusteella pilvipalvelut voidaan luokitella muutamaan päätyyppiin eli pilvipalvelumalleihin (Heino 2010, 50). Yleisimmin jako on tehty kolmeen as-a-service-malliin (aaS). Infrastruktuuriresurssipalveluna (IaaS), alustaresurssipalveluna (PaaS) ja ohjelmistoresurssipalveluna (SaaS). Neljäntenä saatetaan mainita usein Liiketoimintaprosessi palveluna (BPaaS), jolloin yksittäisen palvelun sijasta toimitetaan kokonainen liiketoimintaprosessi pilvipalveluperiaatteiden mukaisesti. Jako kolmeen on usein siis yleisin, muttei kuitenkaan ainoa tapa tarkastella palvelumalleja, esimerkiksi tallennustila palveluna (Storage-as-a-service), tietoturvapalvelut palveluna (Security-as-a-Service) tai viestintä palveluna (Communication-as-a-service) voidaan irrottaa omiksi kokonaisuuksikseen. (Salo 2012, 20–21.)

Pilvipalvelumallit ja käytetyt teknologiat ovat kuitenkin harvoin palvelun käyttäjän kannalta itsessään kiinnostavia tai olennaisia muutoin kuin käyttäjän omaa liiketoimintaa mahdollistavana ja sitä tukevina ja kehittävinä toimintoina. Pilvipalveluilla on vain välinearvoa niitä käyttäville yrityksille, sillä yritysten tavoitteena on pystyä tehostamaan omaa liiketoimintaansa ja saamaan kilpailuetua niiden avulla. Käyttäjän ei tarvitse maksaa kuin vain tarvitsemistaan resursseista, jotka ovat nopeasti skaalautuvia. Ei tarvitse huolehtia investoinneista, kiinteistä laitteistokustannuksista, sovelluksiin tai ylläpitoon liittyvistä kustannuksista tai hankkia omaa osaamista. (Salo 2012, 21.)

2.2.1 Sovellusalusta palveluna

Sovellusalusta palveluna pilvipalvelumallissa asiakkaalle tarjotaan virtuaalinen palvelinympäristö, jonka kapasiteettia ja työkaluja asiakas voi käyttää omien ohjelmiensa kehittämiseen ja testaamiseen (Heino 2010, 51). Tämä mahdollistaa sovelluskehittäjille yksinkertaisemman tavan työskennellä, kun infrastruktuurista ei tarvitse huolehtia ja palveluihin saa usein liitettyä tarvittavia toiminnallisuuksia valmiina moduuleina ja ohjelmointirajapintoina. Valmista alustaa käytettäessä kehitystyö on nopeampaa, tehokkaampaa ja valmis lopputulos on helposti skaalattavissa tarvittavaan kokoon. SaaS-palvelut mahdollistavat myös uusien toimijoiden pääsyn markkinoille ilman suuria aloitusinvestointeja. Kun alustan ylläpitoon ei tarvitse sitoa omia resursseja voivat kehittäjät keskittyä omaan liiketoimintaansa eli uusien ohjelmien ketterään luomiseen ja vanhojen parantamiseen. (Salo 2012, 24–25.)

2.2.2 Sovellukset palveluna

Sovellukset palveluna mallissa yritys ostaa yhden tai useamman sovelluksen pilvipalveluna. Useissa tapauksissa asiakas pääsee käyttämään ohjelmiaan internetselaimen kautta. Sen sijaan, että yrityksen pitäisi ostaa oma lisenssi tiettyä ohjelmaa varten ja tämän jälkeen asentaa jokaiselle työasemalle tarvittava ohjelma on pilvipalveluna ostettu ohjelma käytössä tarvittaessa esimerkiksi aikaperusteisen, käyttäjä- tai konekohtaisen maksun mukaan. Tämän avulla yritys säästyy ylläpidolta ja

hankalalta tarvittavien ohjelmien päivitykseltä. Kun käyttäjä avaa internetin kautta tarvittavan ohjelman, on se aina valmiiksi päivitetty ja käyttövalmis. (Salo 2012, 25–26.)

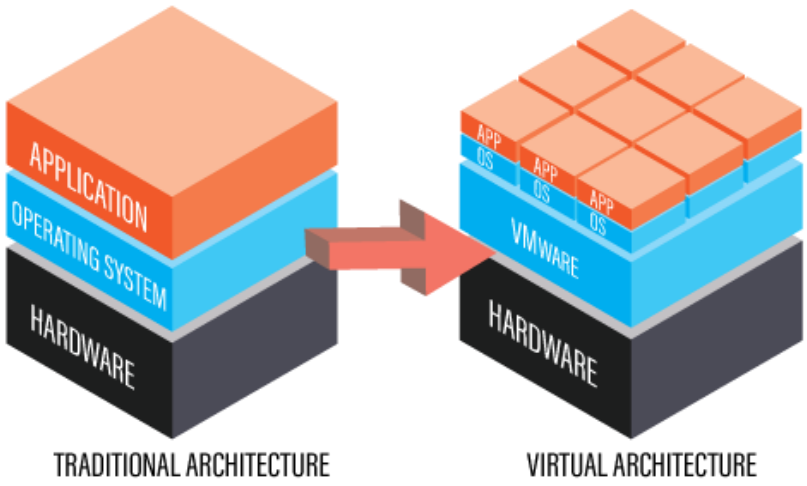
2.2.3 Infrastruktuuri palveluna

Infrastruktuuri palveluna mallissa yritys ostaa pilvipalvelun tarjoajalta joko fyysisiä tai virtuaalisia palvelimia. Yleisesti pilven kautta ostettaviin palvelimiin voi valita tarvittavan määrän teknisiä resursseja tarpeen mukaan ja laskutus menee usein myös valittujen resurssien mukaan. (Heino 2010, 52.) Yritys voi tällöin muokata palvelimia juuri omaan tarkoitukseen sopiviksi, kuten esimerkiksi asentaa tarvittavia ohjelmia pyöritettäväksi pilvi-infrastruktuurin päällä. Oman palvelininfrastruktuurin ylläpito on yritykselle hyvin vaivalloista ja kallista. Alkuinvestointi voi olla hyvinkin suuri, ennen kuin oman palvelinympäristön saa edes käyttöönsä. Tarvitaan omat fyysiset tilat, jossa omia palvelimia voi turvallisesti pitää ja palvelimien ylläpitoon ja huoltoon tarvitaan omaa osaamista. Resurssikapasiteetti on rajallinen ilman uusien fyysisten komponenttien ostamista ja asentamista, minkä vuoksi oman ympäristön skaalautuvuus ei ole kovin nopeaa. Pilvipalveluna ostettu infrastruktuuri ulkoistaa lähes kaikki yllämainitut ongelmat. Palveluntarjoajalla on jo lähtökohtaisesti suuri resurssikapasiteetti, jonka avulla yrityksen tarpeet täyttävän osuuden käyttöönotto on nopeaa. Samalla tulevaisuuden skaalautuvuusongelmista ei tarvitse huolehtia. Tilavuokrakustannuksia tai henkilöstökustannuksia ei synny, kun palvelimille ei tarvitse varata tilaa eikä osaamista niiden ylläpitoon. Tällöin yritys voi keskittyä vain infrastruktuurin käyttöön. (Salo 2012, 22–23.)

2.3 Pilvipalveluiden tekniikoita

Jotta nykyisten pilvipalveluiden tarjoaminen olisi edes mahdollista on tätä ennen tarvittu kehittää useita erilaisia tekniikoita. Näitä ovat muun muassa virtualisointi, tietoliikenne, langattomat yhteydet ja tallennuskapasiteetin siirto pilveen. Edellä mainitut tekniikat eivät ole uusia, alkujaan pilvipalveluita varten kehitettyjä, mutta niiden ja kehittyneen teknologian ansiosta nykyiset pilvipalvelut ovat mahdollisia. (Heino 2010, 58.)

Virtualisoinnilla mahdollistetaan pilvipalvelukapasiteetin helppo, kustannustehokas ja skaalautuva käyttö. Sen avulla voidaan luoda palvelimia ilman nykyisen fyysisen palvelinkapasiteetin kasvattamista. Virtualisoinnissa fyysinen palvelinlaite, eli isäntäkone, jakaa omia teknisiä resurssejaan useammalle palvelimelle hypervisor-ohjelman avulla. Tämä ohjelma mahdollistaa virtualisoidun palvelimen keskustelun fyysisten komponenttien kanssa. Tämän jälkeen hypervisorin päälle voi asentaa virtuaalisia palvelimia nopeasti. Myös tarpeettomien palvelimien poistaminen onnistuu helposti ilman fyysisiin laitteisiin koskemista. Uudelle palvelimelle voi valita käyttöjärjestelmän tarpeen mukaan, eikä sen tarvitse olla sama isäntäkoneen kanssa. Virtualisoinnin avulla tarvittavan alkuinvestoinnin jälkeen yhtä palvelinta kohti tarvittavat kustannukset pienenevät merkittävästi. Uuden palvelimen asennukseen ei tarvita omaa fyysistä laitteistoa vaan se voidaan virtualisoida olemassa olevaan infrastruktuuriin. (Heino 2010, 59–60.) Kuvassa 1 havainnollistetaan perinteisen tietokoneen ja virtuaalisen palvelimen eroa. Fyysiselle koneelle voidaan asentaa kerrallaan vain yksi käyttöjärjestelmä, jonka kautta tietokonetta käytetään. Virtualisoinnin avulla yhdellä fyysisellä laitteella voi olla useita virtuaalisia palvelimia, jotka voivat suorittaa eri prosesseja.



KUVA 1. Palvelimen ja virtualisoidun palvelimen rakennekuva (Cyrbertrol Engineering)

Pilvipalveluiden ominaispiirteisiin kuului mahdollisuus yhdistää näihin lähes millä päätelaitteella tahansa ja tämä tapahtuu useimmiten internetin välityksellä. Pilvipalveluiden yleistymiseen on tietenkin vaadittu tietoliikenteen ja langattomien

verkkojen kehittyminen. Riippuen yrityksen omasta käyttäjämäärästä vanhempikin, hitaampikin internetyhteys voi olla riittävä. Käyttäjäkunnan ollessa suurempi on mahdollista, että vanhempi internetyhteys joudutaan vaihtamaan nopeampaan vaihtoehtoon pilvipalveluiden käytön mahdollistamiseksi. Nopeat langattomat verkkoyhteydet ovat onneksi yleistyneet 2010-luvulla tukemaan kaapeliyhteyksiä ja nykyään niiden kantoalue on jo varsin kattava. Näiden avulla kohtuuhintaisia nettiliittymiä on saatavilla varsin helposti, mikä mahdollistaa pilvipalveluiden käyttöönoton yhä laajemmin. (Heino 2010, 65–71.)

Tietokoneiden yleistyminen ja myöhemmin digitalisaatio on muuttanut ennen paperille painetun tiedon digitaaliseen muotoon. Tätä varten tarvitaan myös digitaalista tallennustilaa. Ongelmaksi osoittautuu, että minne yrityksen tiedostoja tallennetaan, jotta ne olisivat kuitenkin helposti saatavilla useasta eri paikasta, turvassa ja varmuuskopioitu. Jos yrityksellä on omaan lähiverkkoonsa asennettu verkkotallennussijainti, tarvitaan oman sisäverkon ulkopuolelta siihen yhdistämiseen suojattu VPN-yhteys (Virtual Private Network -yhteys). Tämä hieman rajaa käytettäviä päätelaitteita, sillä jokaiselta laitteelta on löydyttävä tarvittava VPN-ohjelma. Yksityistä pilvipalvelua voidaan myös käyttää VPN-yhteyden yli yrityksen sisäisen verkon ulkopuolelta. Suojatun yhteyden kautta käytettävä oma palvelu parantaa tietoturvaa ja kontrollia suhteessa julkiseen pilvipalveluun. Yksityisestä pilvestä pääsee paremmin hallitsemaan ympäristöön avattuja yhteyksiä ja reagoimaan vääriin yhteyksiin. Ulkoistettuun palveluun avattuja yhteyksiä ei pääse hallinnoimaan ilman palveluntarjoajan apua. Julkisesta pilvestä ostettu tallennuskapasiteetti on saatavilla eri paikoista ja eri päätelaitteilla joustavammin. Omiin tiedostoihin pääsee käsiksi yleensä ilman ylimääräisiä ohjelmia. Parantuneet tietoliikenneyhteydet ovat myös osaltaan mahdollistaneet tiedostojen pitämisen pilvessä. Lisäksi kun tallennustila on ostettu pilvipalveluna, kuuluu tähän myös varmuuskopiointi. Näin yrityksen ei tarvitse itse hankkia osaamista ja laitteita tiedostojensa turvalliseen sijoittamiseen. (Heino 2010, 84–85.)

2.4 Pilvipalveluiden edut ja hyödyt

Pilvipalveluista on monenlaista hyötyä yrityksille. Suurimmalle osaa yrityksistä tietotekniikka ei ole osa heidän liiketoimintaansa, vaan se on mahdollistava ja tukeva

osa sitä. Tämän vuoksi tietotekniikalla on omat vaatimuksensa yrityselämässä. Sen kuuluisi olla mahdollisimman edullista, helppoa, nopeaa ja varmaa. Näiden vaatimusten täyttäminen yrityksen omalla tietotekniikalla on hyvin rajallista. Vaaditaan lähtökohtaisesti suuri alkuinvestointi tarvittavien laitteiden hankintaan. (Viswanthan 2017.) Ajan kuluessa näitä laitteita täytyy uusia ja tarvittavat ohjelmat täytyy ostaa erikseen. Lisäksi yritys tarvitsee turvalliset tilat, joihin laitteet voidaan sijoittaa. Kertakustannusten lisäksi oman laiteinfrastruktuurin ylläpitoon kuuluu suuri määrä juoksevia kustannuksia. (Joytsana 2016.) Suuri laitemäärä kuluttaa paljon sähköä ja tuottaa suuren määrän lämpöä, minkä vuoksi laitetiloihin tarvitaan tehokas ilmastointijärjestelmä. Lisäksi ylläpitoon tarvittavan henkilöstön palkkaus nostaa kuluja merkittävästi. (Pritchett 2018.)

Yrityksen omien palvelinympäristöjen kaksintaminen on kallista, mutta jos jokin laite hajoaa, eikä varajärjestelmää ole, saattaa koko yrityksen liiketoiminta pysähtyä kokonaan pitkiksikin ajoiksi. Pilvipalveluiden käyttö on puolestaan varsin varmaa. Palveluntarjoajilla on käytössään tarvittavat laitteet ja osaaminen nostaakseen luotettavuutensa korkealle tasolle ja ongelmatilanteissa varajärjestelmiä saadaan nopeasti käyttöön. Tällöin ongelmatilanteiden vaikutukset yritysten toimintaan jäävät useimmiten pieniksi. On kuitenkin hyvä ottaa huomioon, että jos yrityksellä on kymmenen käyttäjää ja heidän työntekonsa keskeytyy kymmeneksikin minuutiksi menee yritykseltä hukkaan 100 minuuttia työaikaa. Pilvipalveluiden käyttökatkot vaikuttavat kaikkii käyttäjiin, kun oman järjestelmän ongelmat eivät välttämättä vaikuta kaikkiin käyttäjiin tai työtehtäviin. (Pritchett 2018.) Palveluntarjoajien sopimusehdoissa mainitaan SLA-sopimus (palvelutasosopimus), joka on usein jotain 99,95% ja 99,99% väliltä. Tällä tarkoitetaan, että palvelu on käytettävissä esimerkiksi 99,95% ajasta. (Salo 2012, 39.) Lisäksi palveluntarjoajien infrastruktuuri on jatkuvasti hyvin tarkan seurannan kohteena, jolloin mahdollisiin ongelmiin pystytään jo reagoimaan ennen niiden syntymistä (Joytsana 2016.) On myös hyvä muistaa, etteivät omat järjestelmätkään ole täysin varmoja ja käyttökatkoja tapahtuu niissäkin. Pilvipalveluissa käyttökatkot ovat kuitenkin suhteellisen harvinaisia ja lyhyitä. (Cox 2017.)

Nopeus ja joustavuus ovat pilvipalveluiden eräitä suurimpia hyötyjä. Tietokoneresurssien ottaminen käyttöön tai pois käytöstä ilman pitkiä viiveitä mahdollistaa palveluiden huolettoman käytön. (Pritchett 2018). Useimmiten muutokset tapahtuvat automaattisesti ja huomaamatta. Suurten käyttäjäpiikkien aikaan

laitekapasiteettia saadaan nopeasti käyttöön eikä käyttökatkoja pääse syntymään. Toisaalta kun käyttöpiikki on, ohi voidaan resurssien määrää skaalata nopeasti alaspäin ja näin vähennetään syntyviä kustannuksia. (Salo 2010, 45.)

Pilvipalvelut tuovat myös huolettomuutta ja ajankäytön tehostamista. Yrityksen käyttäjät ovat harvoin osaavia tietotekniikan asiantuntijoita ja ongelmien esiintyessä aikaa saattaa kulua paljonkin niiden ratkaisemiseen. Pilvipalveluita käytettäessä käyttäjän ei tarvitse huolehtia ohjelmien päivittämisestä, tietoturvasta tai niihin liittyvistä tukitehtävistä vaan voi paremmin keskittyä omaan työskentelyynsä. Tarvittavat tukitoimet tapahtuvat näkymättömissä taustalla ja aina kun käyttäjä yhdistää tarvitsemaansa palveluun on tämä heti käyttövalmis. (Salo 2010, 47.)

On otettava toki huomioon, etteivät pilvipalvelut poista tietotekniikkaan liittyviä ongelmia. Ongelmat vain ulkoistetaan palveluntarjoajalle, joka on velvollinen ehkäisemään ja korjaamaan ongelmat niiden esiintyessä. Erona on, että pilvipalveluntarjoajat ovat itse oman alansa ammattilaisia, joten heillä on paremmat taidot ja välineet ongelmien ratkaisemiseen kuin palvelun käyttäjillä. Ongelmat eivät siis katoa, jos yritys ulkoistaa tietotekniikkaan liittyvät asiat pilvipalveluntarjoajalle, vaan nekin siirtyvät ulkoistuksen yhteydessä.

2.5 Pilvipalveluiden riskit ja huolenaiheet

Pilvipalveluihin liittyy myös useita huolenaiheita. Suurimmat näistä liittyvät palveluntarjoajan luotettavuuteen. Kun vähintäänkin osa yrityksen datasta siirretään tai kopioidaan omista laitteista ja omasta hallinnasta kolmannelle osapuolelle herää usein huoli onko yrityksen data aidosti turvassa ja vain oikeiden henkilöiden saatavilla. (Pritchett 2018.) Palveluntarjoajat myös harvoin antavat juurikaan tietoja omien järjestelmiensä rakenteesta, tai edes omien palvelinsaliensa maantieteellisestä sijainnista. Toisaalta läpinäkymättömyys tuo osaltaan turvallisuutta, kun palvelinsaleihin ei pääse kuka vain tutustumaan. (Salo 2012, 37–38.)

Epävarmuutta pilvipalveluista tuo kontrollin vähäisyys. Omasta järjestelmästä on helppo esimerkiksi nähdä, kuka on viimeksi tehnyt muutoksia johonkin dokumenttiin, mutta pilvipalvelusta tuon tiedon hakeminen on usein hankalampaa ja usein myös

mahdotonta ilman palveluntarjoajan asiakaspalvelijan apua. Pilvipalveluiden luotettavuutta on pyritty parantamaan muun muassa erilaisten sertifikaattien ja laatustandardien avulla mutta nämäkään eivät hälvennä kaikkia huolia. Yrityksen on näissäkin tapauksissa varmistettava, että palvelunehtosopimus velvoittaa palveluntarjoajan riittävän huolelliseen ja tarkkaan tietojen käsittelyyn. (Salo 2012, 44.)

Pilvipalvelutkaan eivät ole täysin riskittömiä mutta niiden tuomat hyödyt voittavat useimmiten haitat. Monen yrityksen mielestä taloudelliset säästöt, saavutettavuus ja varmuuskopioinnit ovat arvokkaampia kuin niihin liittyvät riskit. (Pritchett 2018.) Riskejä ei kuitenkaan kannata unohtaa ja luottaa sokeasti palveluntarjoajaasi, vaan riskeihin kannattaa myös varautua. Esimerkiksi datan varmuuskopioinnista kannattaa varmistua, sillä tallennustila on varsin halpa resurssi. Kannattaako kaiken yrityksen datan olla vain pilvessä, vai pidetäänkö jotkin kopiot itsellä? Onko pilvipalveluntarjoajalla yrityksen data varmuuskopioituna useampaan paikkaan ja onko data salattu mahdollisen tietomurron varalta? Datan turvallisuuden lisäksi kannattaa myös miettiä miten yrityksessä toimitaan, jos esimerkiksi tulee suurempi pilvipalvelun käyttökatkos. Voidaanko töitä jatkaa muutoin ja jos ei, niin miten palveluntarjoaja varmistaa, että palvelu saadaan mahdollisimman nopeasti takaisin käyttöön. Pienelläkin varautumisella voidaan ehkäistä epävarmoja tilanteita pilvipalveluita käytettäessä, eikä palveluiden riskejä kannata kokonaan unohtaa, vaikka ne häviävätkin niiden tuomille hyödyille. (Salo 2012, 46–47.)

On myös hyvä muistaa, että pilvipalveluiden tarjoajien palvelut ovat hyvin riippuvaisia niiden maineesta. Media uutisoi mahdollisista tietomurroista hyvin laajasti, minkä vuoksi palveluntarjoajilla on suuri intressi parantaa palveluitaan turvallisimmiksi ja tehdä ongelmista tiedottamisesta läpinäkyvää ja nopeaa. Tämän avulla pilvipalveluiden käyttäjät voivat olla varmoja, että saavat tiedon mahdollisista väärinkäytöksistä tai tietomurroista. (Salo 2012, 38.)

Pilvipalvelun käyttö on myös riippuvainen internetyhteydestä. Vaikkakin erilaiset langattomat verkkoyhteydet ovat parantuneet viime vuosina voivat ne silti toimia vaihtelevasti verkon kuormituksen mukaan. Tarvitaan siis tasainen yhteys pilvipalveluun, jotta käyttö on tasaista ja varmaa. Jos internet yhteys pätkii tai joudutaan verkon katvealueelle estyy pilvipalvelun käyttö ja samalla työn teko. (Viswanthan 2017.)

Pilvipalveluntarjoajat ovat myös selkeitä hyökkäyskohteita verkkorikollisille. Suurilla pilvipalveluntarjoajilla voi olla lukemattomia yritysasiakkaita, keiden data on arvokasta. Tällainen kohde on paljon houkuttelevampi, kuin yksittäisen yrityksen oma sisäverkko. Pilvipalveluun ulkoistettaessa on siis otettava myös huomioon suurempi todennäköisyys tulla epäsuoran hyökkäyksen kohteeksi. Erilaiset palvelunestohyökkäykset ovat myös yleisiä pilvipalveluja vastaan, mitkä saattavat estää tai hidastaa palvelun käytön. (Viswanthan 2017.)

Pilvipalveluiden osalta on otettava myös huomioon teknisen tuen saanti. Jos yrityksellä on oma infrastruktuuri käytössä heillä on usein myös paikalla oleva tuki, joka voi auttaa paikan päällä ongelmatilanteissa. Kun tietotekniikkaa ulkoistetaan pilvipalvelulle, siirtyy tuki myös kauemmaksi. Ongelmatilanteissa joudutaan usein keskustelemaan sähköpostin tai puhelimen välityksellä, mikä saattaa osaltaan vaikeuttaa ongelmien ratkaisua.

3 TIETOTURVA

3.1 Mitä tietoturvalla tarkoitetaan?

Muutamassa vuosikymmenessä käytössämme on lukuisia sähköisiä palveluja, joita käytämme päivittäin. Ennen varasimme hotellimajoittumisia puhelimitse ja ostimme niin elokuva-, kuin junaliput vasta elokuvateatterista tai juna-asemalta. Nykyään tuo kaikki tapahtuu jo suurelta osin internetissä. Sähköiset palvelut helpottavat suuresti arkeamme, mutta ne voivat toimia myös meitä vastaan, jos palveluntarjoajat eivät pidä palveluistaan huolta, emmekä me käyttäjät osaa käyttää niitä oikein. Tämän vuoksi tietoturvan kuuluisi olla 2000-luvun kansalaistaito. (Järvinen 2012, 10.)

Tietoturva on laaja aihe, johon kuuluu useita osa-alueita. Kaikelle toiminnalle on kuitenkin nähtävissä pyrkimys kolmeen tavoitteeseen. Sähköisesti liikkuvan tiedon pitäisi pysyä aina luottamuksellisena, jolloin datan kuuluisi olla vain tarkoitetun ihmisryhmän nähtävillä. Tietoihin pääsyä hallitaan käyttäjien tunnistamisella, käyttäjäoikeuksien rajoituksilla, sekä datan salaukseen käytettävillä algoritmeilla. Sähköisessä muodossa olevan tiedon pitää säilyä myös eheänä. Tiedostoihin saa siis kohdistua vain oikeutettuja muutoksia, eikä niihin saa tapahtua sisällön muutoksia esimerkiksi siirron yhteydessä. Tätä pyritään varmistamaan tiedostojen salaamisella. Tietojen pitää myös olla saatavilla, koneiden käytettävissä ja palveluiden toimia tarvittaessa. Tämän täydellinen saavuttaminen on jo hyvin haasteellista, mutta tähän kuitenkin pyritään parhaan osaamisen mukaan. (Järvinen 2012, 10.) Tietoturvan piiriin voidaan ajatella kuuluvan tietoliikenne-, laitteisto-, ohjelmisto- ja tietoaineistotoiminnan turvallisuus. Suomessa teleyritysten yleisiä viestintäverkkojen tietoturvallisuutta valvoo viestintävirasto. (Viestintävirasto 2013.)

3.2 Todentaminen

Todentaminen on yksi kaikkein tärkeimmistä asioista tietoturvasta puhuttaessa. Voimme pyrkiä tekemään turvallisia teknisiä järjestelmiä, jotka käyttävät hyväkseen monimutkaisia salausalgoritmeja ja virustorjuntoja saastuneiden tiedostojen nappaamiseen, mutta se kaikki on turhaa, jos verkkorikollinen pääsee kävelemään järjestelmään sisälle suoraan etuovesta. Jokainen käyttäjä pitää siis pystyä tunnistamaan

juuri oikeaksi henkilöksi kenellä on oikeudet päästä järjestelmään sisälle. Tästä syystä useat tietoturvaongelmat saavat alkunsa pohjimmiltaan todentamisen ongelmista, eikä niinkään teknisistä puutteista. (Järvinen 2012, 12.) Todentaminen tapahtuu siis lähes kaikissa niissä tilanteissa, kun ihminen yhdistää johonkin palveluun. Perinteisesti käyttäjän tunnistaminen on koostunut käyttäjätunnuksen ja salasanan yhdistelmästä. Käyttäjän tunnistamiseen suositellaan kaksivaiheista tunnistautumista, missä käyttäjätunnuksen ja salasanan lisäksi kysytään vielä esimerkiksi sähköpostilla tai tekstiviestillä lähetettävä kertakäyttöinen salasana. (Rouse & Haughn 2014.)

3.3 Salasana ja salasanakäytännöt

Salasana on jono vapaasti valittavia merkkejä, mitä käytetään käyttäjän todentamisen yhteydessä. Salasana asetetaan usein vähimmäis- ja toisinaan myös enimmäispituus. Se voi sisältää kirjaimia, numeroita ja erikoismerkkejä. (Rouse & Bacon 2017.) Salasana ei kuitenkaan ole täysin ongelmaton. Se on hyvin riippuvainen itse käyttäjästä, sillä salasanoja ei sääntöjen ja salasanakäytänteidenkään avulla pystytä tekemään täysin aukottomiksi. Käyttäjä voi unohtaa salasanansa, mikä aiheuttaa ongelmia palvelun käytössä. Toisin kuin kulkukortin tai avaimen, salasanan voi luovuttaa sähköpostilla tai puhelimitse. Tämä tapa ei ole suositeltava, sillä salasanan paljastuminen ulkopuoliselle henkilölle aiheuttaa vakavan tietoturvariskin ja yrityksen tiedostot ovat näin vapaasti kopioitavissa väärään käyttöön. (Järvinen 2012, 112–113.)

Käyttäjille asetetaan usein monenlaisia salasanavaatimuksia. Salasanojen pitäisi olla riittävän pitkiä ja sisältää erikoismerkkejä, niitä pitäisi vaihtaa säännöllisesti, niitä ei saisi kirjoittaa muistiin ja jokaiseen käytettävään palveluun pitäisi keksiä oma salasana. Yllä mainitut vaatimukset ovat hyviä, mutta niissä on yksi ongelma. Edes vaatimusten keksijä ei pysty noudattamaan näitä kaikkia. (Järvinen 2012, 114.)

3.3.1 Salasanan riittävä pituus

Salasanan pituuden pitäisi olla riittävä. Mitä tällä tarkoitetaan? Salasanan pituudella pyritään estämään niin sanottuja brute-force-hyökkäyksiä. Siinä hyökkääjän tietokone tai yleisemmin suuri ryhmä tietokoneita käy läpi merkki merkiltä erilaisia

merkkiyhdistelmiä salasanan selvittämiseksi. Yleisesti palveluissa vaaditaan vähintään kahdeksan merkkiä pitkiä salasanoja, mutta jokainen ylimääräinen merkki kasvattaa salasanan murtamiseen kuluvaa aikaa 28-kertaiseksi. Salasanan pituutta kannattaa siis ennemmin kasvattaa kuin muuttaa jokin kirjain erikoismerkiksi, vaikka pitkä merkkijono hankaloittaa salasanan muistamista ja nostaa unohtamisen todennäköisyyttä. (Järvinen, 2012, 114–116.)

3.3.2 Salasanan vaihtaminen

Salasanan vaihtamisella pyritään korjaamaan tilanne, että salasana on paljastunut ulkopuoliselle, mutta tämä on jäänyt huomaamatta käyttäjältä. On toisaalta hankala nähdä salasanan vaihtamisen hyöty. Jos salasana paljastuu, kestää vain muutama minuutti, kun kaikki tärkeät tiedot on jo kopioitu muualle. Tällöin kuukauden päästä vaihdettava salasana ei juurikaan auta. Toki sellaisessa tilanteessa salasanan vaihdosta on hyötyä, jos salasanan kaapannut taho jää vakoilemaan käyttäjän tietokonetta tai palvelua pidemmäksi aikaa. Toisaalta tunnuksen samanaikainen käyttö kahdesta eri IP-osoitteesta pitäisi soittaa yrityksen verkossa hälytyskelloja. Jos salasanan vaihtamisen väli on esimerkiksi kolme kuukautta, niin kannattaa miettiä onko vaihtamispakolla saatava lisäturva vaivan arvoinen. (Järvinen 2012, 116.)

3.3.3 Salasanan muistaminen

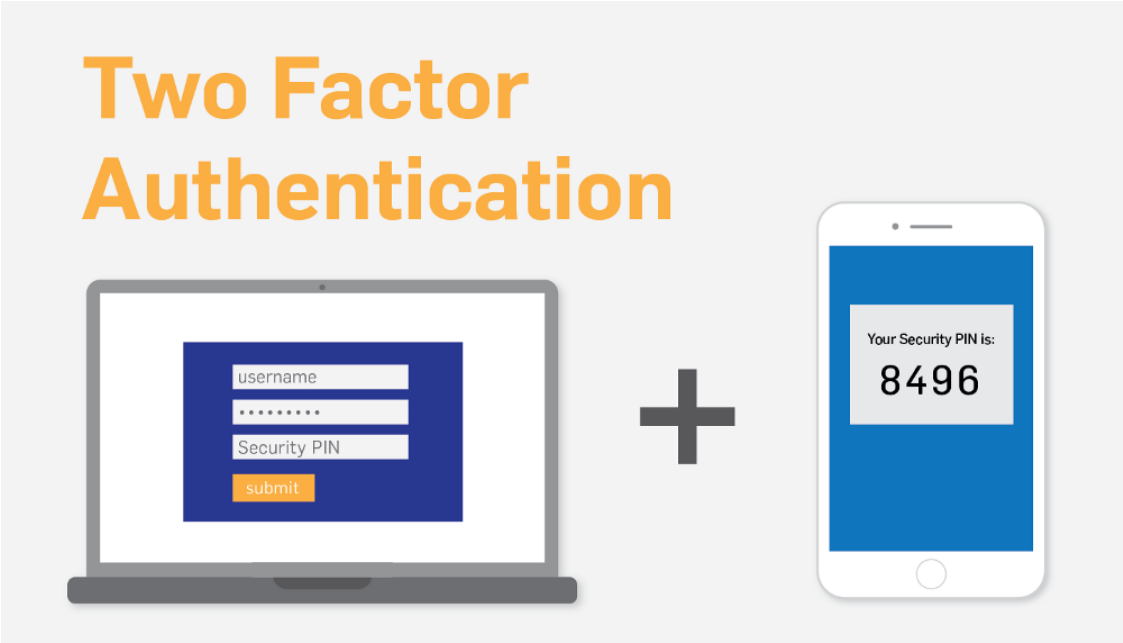
Lähtökohtaisesti oletetaan, että salasana muistetaan aina ulkoa eikä sitä saa kirjoittaa mihinkään. Nykypäivänä sähköisten palveluiden lukumäärä nousee jo useisiin kymmeniin, niin on mahdotonta olettaa käyttäjän muistaa nämä kaikki ulkoa. Unohtunut salasana on yksi kaikkein suurimmista riskeistä. Jos henkilö soittaa yrityksen tai palvelun tekniseen tukeen ja pyytää salasanansa nollaamista on kyseisen henkilön henkilöllisyyden varmistaminen todella vaikeaa. Salasanalla pyritään nykypäivän verkostoituneessa maailmassa estää verkon välityksellä tulevat murtoyritykset. Tätä ajatellen on turvallisempaa kirjoittaa pitkä salasana lapulle ja piilottaa se esimerkiksi näppäimistön pohjaan, kuin käyttää helposti muistettavaa ja ennalta arvattavaa salasanaa palveluissaan. (Järvinen 2012, 117–118.)

3.3.4 Jokaiseen palveluun oma salasana

Neljäs salasanavaatimus on ehkä kaikkein tärkein. Jokaisessa palvelussa pitäisi käyttää eri salasanaa. Jos jonkin palvelun salasana paljastuu ulkopuoliselle kyseisellä salasanalla ei pääse kuin yhteen paikkaan. Tällöin vahinkojen laajuutta saa helposti rajattua. Tämä vaatimus on tietenkin hyvin vahvasti yhteydessä salasanojen muistamiseen. Kun palveluita on käytössä useita kymmeniä ja jokaiseen pitäisi käyttää omaa vahvaa salasanaansa, on käyttäjällä suuri työ hallinnoida niitä. (Järvinen 2012, 118.)

3.4 Kaksivaiheinen tunnistus

Kaksivaiheinen tunnistus on turvallisuus prosessi, missä käyttäjä syöttää kaksi tunnistautumistapaa todentaakseen henkilöllisyytensä (Rouse & Cobb 2016). Vaikka hyökkääjä saisikin urkittua käyttäjän salasanan ei hän pääse kirjautumaan palveluun sisälle. Kun kaksivaiheinen tunnistus on otettu käyttöön käyttäjätunnuksen ja salasanan syötön jälkeen palvelu lähettää ennalta määriteltyyn puhelinnumeroon tai sähköpostiosoitteeseen kertakäyttöisen salasanan. Jotta hyökkääjä pystyisi tämän murtamaan pitäisi hänen urkitun käyttäjätunnuksen ja salasanan lisäksi varastaa käyttäjän puhelin ja todennäköisesti tietää myös sen näppäinlukon salasana, jossa hän pääsee käsiksi kertakäyttöiseen salasanaan. Tämä nostaa jo murtautumisen vaikeusastetta huomattavasti suuremmaksi. (Järvinen 2012, 144.) Toki se myös lisää käyttäjän sisäänkirjautumisen vaivallisuutta, mutta uskon, että se on saavutetun lisäturvallisuuden arvoista. Kuvassa 2 havainnollistetaan kaksivaiheisen tunnistuksen käyttöä. Käyttäjä kirjautuu sisälle palveluun syöttämällä ensin käyttäjätunnuksensa ja salasanansa, minkä jälkeen hän saa vielä puhelinnumeroonsa, esimerkiksi tekstiviestillä, kertakäyttöisen salasanan, joka syötetään palveluun.



Kuva 2. Kaksivaiheinen tunnistus lisää tilin turvallisuutta. (Shameer)

4 SALASANAPALVELUN ASENTAMINEN MAGIC CLOUD OY

4.1 Toimeksiantajan esittely

Opinnäytetyö tehtiin Magic Cloud Oy:n toimeksiannosta. Magic Cloud Oy on Pirkanmaalla toimiva, yritysasiakkaille pilvipalveluja tarjoava ICT-alan pk-yritys. Toimeksiantajan pääliiketoimintaa on tarjota erilaisia sovellukset palveluna -mallin mukaisia virtuaalisia palveluja, kuten virtuaalityöpöytiä ja -ohjelmia. Toimeksiantaja on erikoistunut erilaisten kirjanpito ja palkanlaskentaohjelmien tarjoamiseen pilvipalveluna, joiden lisäksi asiakkaille tarjotaan pilvestä muun muassa tallennuskapasiteettia ja sähköpostipalveluja. Toimeksiantajan kilpailuvalttina on tarjota Suomessa toimiville yritysasiakkailleen kotimaista pilvipalvelua. Toimeksiantajan palvelinsalit ja asiakaspalvelu sijaitsevat Suomessa, joten asiakkaiden data on maantieteellisesti hyvinkin lähellä ja helposti saatavilla verrattuna suuriin pilvipalvelun tarjoajiin. Näiden palvelinsalit voivat olla hyvinkin kaukana ja Suomessa ei välttämättä ole omaa asiakaspalvelukeskusta laisinkaan.

4.2 Alkuasetelma

Useassa tapauksessa asiakkaan käyttäjän työnteko tapahtuu suurelta osin Magic Cloudin tarjoamassa pilvipalveluympäristössä. Palveluun yhdistäminen tapahtuu, kuten lukuisiin muihinkin palveluihin, käyttäjätunnuksen ja salasanan avulla. Tilanteessa, jossa käyttäjä ei pääse kirjautumaan palveluun sisälle esimerkiksi vanhentuneen tai unohtuneen salasanan takia työnteko estyy suurilta osin. Vastaavassa tilanteessa käyttäjän on otettava yhteyttä palveluntarjoajan asiakaspalveluun nollatakseen salasanansa ja näin päästäkseen jatkamaan työntekoaan. Tämä vie sekä käyttäjän, että asiakaspalvelun työaikaa, minkä voisi käyttää tuottavaan työhön. Toimeksiantajalla ei ole tarkkaa tietoa kuinka paljon tekniseltä tuelta menee aikaa salasanojen nollaamiseen, mutta henkilökohtaisella kokemuksella voin sanoa, että niitä tulee päivittäin. Lisäksi tilanne synnyttää tietoturvaongelman, sillä toimeksiantajan asiakaspalvelija ei pysty puhelimessa varmistamaan soittajan henkilöllisyyttä. Salasanan tarkoitus on juuri todentaa käyttäjän henkilöllisyys, joten salasanansa unohtaneen soittajan henkilöllisyys on todennettava muilla keinoin. Toimeksiantajalla on joidenkin käyttäjien osalta otettu

ylös turvakysymyksiä, mutta näiden vastaukset saattavat helposti unohtua käyttäjältä tai olla helposti arvattavissa sosiaalisen median avulla.

Tätä varten toimeksiantaja asentaa tuotantoympäristöönsä salasanapalvelun. Palvelun avulla käyttäjät voivat itse nollata salasanansa ilman asiakaspalvelun apua. Käyttäjän todentaminen tapahtuu joko tekstiviestillä tai sähköpostilla lähetettävällä kertakäyttöisellä salasanalla. Käyttäjät voivat myös itse päivittää tietojaan palvelun kautta, jolloin käyttäjistä on ylhäällä ajankohtaiset työpuhelinnumerot ja sähköpostiosoitteet. Palvelun avulla käyttäjät pääsevät nopeammin palaamaan töihinsä ja asiakaspalvelu voi keskittyä tuottavampaan työhön. Lisäksi tietoturvaongelmat vähenevät, kun käyttäjän henkilöllisyyden todentamiseen on käytettävissä turvakysymystä varmempi ja turvallisempi keino.

4.3 Tekninen toteutus

Aloitin asennustyön teknisellä palaverilla toimeksiantajan kanssa, jossa hahmottelimme rakennettavaa alustaa palvelun käyttöönottoa varten. Palaveriin osallistui minun lisäkseni Magic Cloud Oy:n toimitusjohtaja sekä järjestelmäarkkitehti. Päätimme, että tietoturvallisuussyistä haluamme rakennettavan palvelun olevan eriytetty muusta tuotantoympäristöstä ja että palvelu keskustelee vain ja ainoastaan tarvittavien järjestelmien kanssa. Palvelun tärkeimmäksi ominaisuudeksi nostimme mahdollisuuden lähettää kertakäyttöisiä salasanoja puhelimeen lähetettävällä tekstiviestillä ja tarvittaessa sähköpostilla. Käyttäjät ottavat yhteyden palveluun suojatulla internet yhteydellä.

Palvelun asentamista varten toimeksiantajan tuotantoympäristöön perustettiin oma VLAN (virtuaalilähiverkko), joka oli erotettu muusta tuotantoympäristöstä. Virtuaalilähiverkko on muusta lähiverkkoympäristöstä eriytetty looginen lähiverkko. Samassa VLAN:ssa olevat laitteet keskustelevat keskenään, kuin ne olisivat kiinnitetty samaan fyysiseen verkkoon. Tämän jälkeen asensin virtuaalipalvelimen salasanapalvelun asentamista varten. Virtuaalipalvelin asennettiin Windows Server 2016 käyttöjärjestelmällä ja virtuaalipalvelin asetettiin käyttämään sitä varten perustettua VLAN:ia. VLAN:sta avattiin pääsy toimeksiantajan domainiin, eli toimialueeseen, jotta palvelin pystyisi liittymään siihen ja keskustelemaan Active Directoryn kanssa salasanojen resetointia varten. Palvelimelle asennettiin

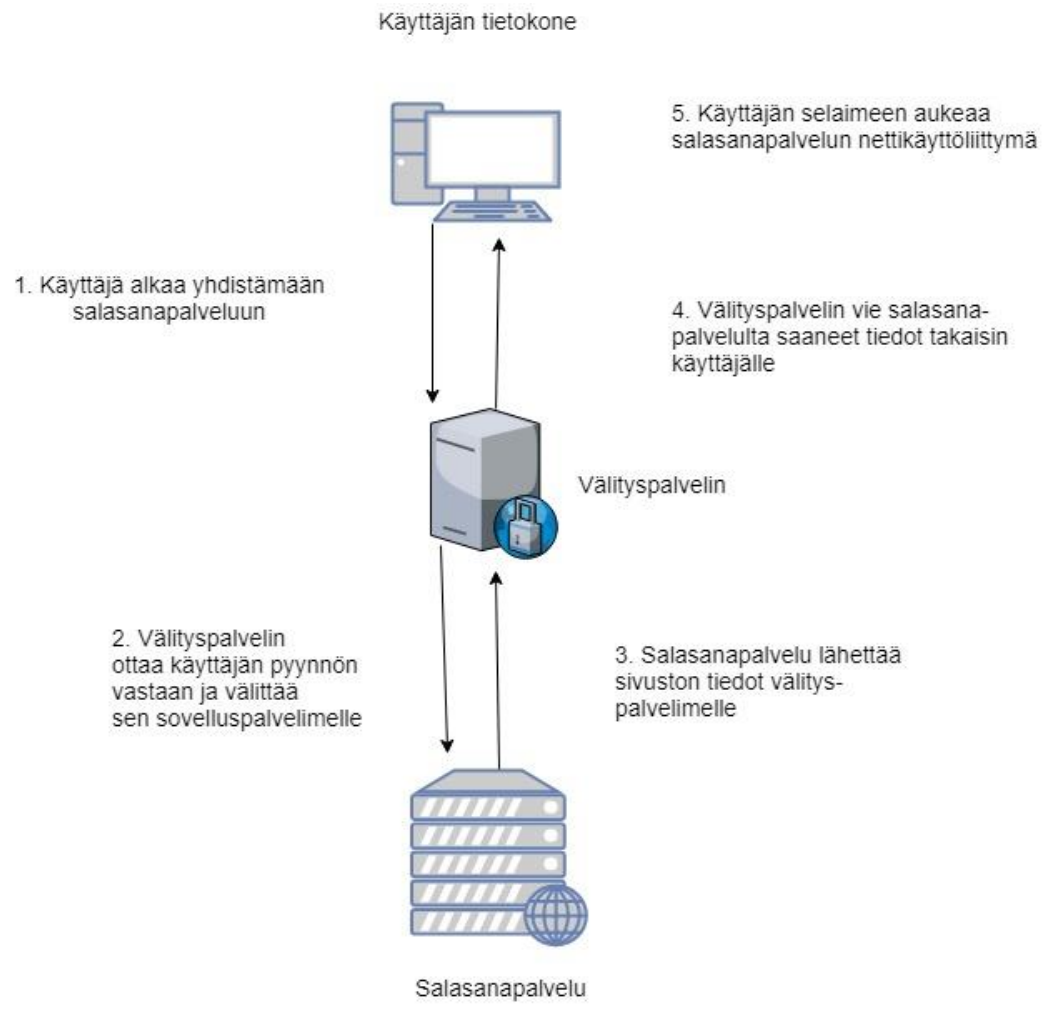
virustorjuntaohjelma, sekä mahdollistettiin Windows päivitysten asentaminen toimeksiantajan WSUS-palvelimelta (Windows Server Update Services). WSUS on työkalu, jonka avulla palvelinympäristön ylläpitäjä voi määrittää, mitä päivityksiä heidän laitteensa saavat. Kun palvelin oli käyttövalmis, aloitin salasanapalvelun asentamisen.

Asennettava salasanapalvelu oli ManageEnginen ADSelfService Plus. Palvelu oli valittu jo ennen opinnäytetyöprosessin alkua, erään ammattikorkeakoulun kurssin projektin lopputuloksena. Projektissa vertailtiin keskenään muutamia salasanapalveluita ja niistä koottiin raportti, jossa esitettiin kyseisen palvelun soveltuvan parhaiten toimeksiantajan vaatimuksiin. Asennus tapahtui ManageEnginen nettisivuilta haettavan asennustiedoston avulla. Asennuksen yhteydessä palvelu yhdisti toimeksiantajan domainiin ja synkronoi sen käyttäjätunnukset palveluun. Tämän jälkeen palvelun kautta pystyi päivittämään käyttäjätunnusten tietoja, vaihtamaan tai nollaamaan salasanoja.

Kun palvelun toimivuus oli varmistettu, aloin selvittää tekstiviestillä lähetettävän kertakäyttöisen salasanan toimintaa. Toimeksiantajalla oli entuudestaan oma SMS-välityspalvelu (Short message service, eli tekstiviesti) käytettävissään, jota halusin käyttää tekstiviestien lähettämiseen. Salasanapalvelun VLAN:sta täytyi ensin avata verkkoyhteys SMS-välityspalveluun. Kun yhteys oli avattu, salasanapalvelun asetuksista tarvitsi määritellä tarvittavat asetukset. SMS-välityspalvelu käyttää tekstiviestien lähettämiseen erilaisia parametreja. Asetuksista sai valita sopivimman protokollan, jolla viesti lähetettiin palvelimelta välityspalveluun. Toimeksiantajalla oli käytössään http:nä (hypertext transfer protocol) lähetettävä viesti, joten katsoin parhaaksi yrittää ensimmäisenä tätä. Http on siis protokolla, mitä nettisivut käyttävät tiedonsiirtoon. Asetin palvelun lähettämään tekstiviestien parametrit välityspalveluun http-muodossa. Viesti koostuu vastaanottajan puhelinnumerosta, välityspalvelun käyttäjätunnuksesta ja salasanasta, sekä itse tekstiviestin sisällöstä. Kopioin http-parametrejä toimeksiantajan jo käytössä olevista parametreistä ja sain tällä menetelmällä tekstiviestin lähettämisen onnistumaan.

Kun SMS-viestien lähettäminen onnistui, aloitin http yhteyden avaamisen internettiin. Tähän mennessä palveluun pääsi yhdistämään vain virtuaalikoneelta. Salasanapalvelun dokumentointiin tutustuessani tulin johtopäätökseen, että internettiin yhdistäminen kannattaa tehdä välityspalvelimen kautta. Sen tarkoituksena on tuoda lisäturvaa

palvelun käyttöön. Kun käyttäjä yhdistää salasanapalveluun internetselaimen kautta, hän normaalisti ottaisi suoraan yhteyden virtuaalipalvelimeen. Kun käyttäjän ja palvelimen väliin asetetaan välityspalvelin, käyttäjän internetselain yhdistääkin siihen. Tämän jälkeen välityspalvelin yhdistää salasanapalvelun virtuaalipalvelimeen ja vie sieltä saadun tiedon takaisin käyttäjälle. Tässä tapauksessa käyttäjä ei ikinä yhdistä suoraan palveluun, vaan luulee keskustelevansa koko ajan vain välityspalvelimen kanssa. Tämä nostaa palvelun turvallisuutta, kun itse salasanapalvelin pysyy välityspalvelimen takana suojassa. Kuvassa 3 havainnollisetetaan salasanapalveluun yhdistämisen eri vaiheet. Salasanapalvelun nettiliikenne kulkee siis aina välityspalvelimen kautta.



Kuva 3. Välityspalvelimen käyttötarkoitus

Välityspalvelimen jälkeen minun tarvitsi suojata palveluun yhdistämiseen käytettävä http yhteys SSL-sertifikaatilla (Secure Sockets Layer). Sertifikaatin avulla käyttäjän nettiliikenne verkkosivulle on salattu ja vaikka hyökkääjä pääsisi vakoilemaan verkkoliikennettä ei tämä pääse lukemaan verkkoliikennettä. Tämä on erityisen tärkeää

nettisivuilla, missä käyttäjä käyttää esimerkiksi pankkitunnuksia tai salasanoja. Pidin toimeksiantajan järjestelmäarkkitehdin kanssa uuden palaverin SSL-sertifikaatin implementoinnista, missä tutkimme sertifikaatin käyttöä salasanapalvelun kanssa. Valmiin SSL-sertifikaatin liittäminen ei ollutkaan aivan niin yksinkertaista, kuin olin ajatellut. Palvelun kautta generoitu sertifikaattipyyntö ei ollut yhteensopiva toimeksiantajan CA:n (Certificate Authorityn) kanssa, joten en saanut luotua SSL-yhteyttä. CA jakaa digitaalisia sertifikaatteja, joiden avulla voidaan salata esimerkiksi nettisivuja. Tutkin tämän jälkeen saako jo olemassa olevan tähtisertifikaatin yhdistettyä salasanapalveluun ja suojata palvelun http-yhteys. Tähtisertifikaatti on siis domainille annettu sertifikaatti, jonka avulla voidaan suojata myös aliverkontunnus. Sertifikaatilla *magiccloud.fi voidaan esimerkiksi suojata osoite salasana.magiccloud.fi. Sain sertifikaatin lopuksi toimimaan käyttäen toimeksiantajan tähti-sertifikaattia. Lisäsimme myös DNS:ään (nimipalvelimeen) tietueen salasanapalvelun nettisivulle. DNS-palvelin kääntää verkko-osoite IP-osoitteeksi ja toisinpäin. Tämän avulla palvelun nettikäyttöliittymään pääsi yhdistämään verkko-osoitteen avulla.

5 POHDINTA

Opinnäytetyön lähtökohtana oli kehittää Magic Cloud Oy:n asiakaspalvelua mahdollistamalla unohtuneen, tai vanhentuneen salasanan vaihtaminen ilman teknisen tuen apua. Lisäksi työn tavoitteena oli tutkia käyttäjän henkilöllisyyden todentamiseen liittyviä tietoturva-asioita ja ottaa ne huomioon salasanapalvelun käyttöönotossa. Lopputuloksena oli toimeksiantajan tuotantoympäristöön asennettu salasanapalvelu, joka vastasi näitä tavoitteita. Asennetun palvelun avulla salasanan vaihtaminen onnistuu nopeasti ja turvallisesti, eikä käyttäjältä tai toimeksiantajan teknisen tuen työntekijältä kulu työaikaa salasanan vaihtoon. Tämä parantaa sekä asiakasyrityksen, että toimeksiantajan työn tuottavuutta. Lisäksi toimeksiantajan salasananvaihtoprosessia saatiin kehitettyä turvallisemmaksi, kun käyttäjien henkilöllisyys saadaan paremmin todennettua tilanteissa, jossa salasana on unohtunut tai vanhentunut.

Opinnäytetyön teoreettinen osuus tukee käytännön työtä hyvin. Toimeksiantajan liiketoiminta keskittyy erilaisten pilvipalveluiden tarjoamiseen yritysasiakkaille ja salasanpalvelun asennettiin heidän tuotantoympäristöön. Näin ollen tutkin, mitä pilvipalveluilla tarkoitetaan, mihin yritysasiakkaat niitä käyttävät ja mitä hyötyjä ja haittoja pilvipalveluihin liittyy. Pilvipalveluiden on tärkeää olla käytettävissä juuri silloin kun niitä käyttäjä tarvitsee. Jos käyttäjän pilvipalvelun salasana on hukassa, estyy hänen työntekonsa. Pilvipalveluiden lisäksi tutkin tietoturvallisuuteen ja etenkin käyttäjän todentamiseen liittyvää aineistoa. Tätä tausta-aineistoa käytin suunnitellessani palvelun salasananvaihtoprosessia ja mitä todentamistapoja käytetään, kun salasana ei ole käytettävissä.

Salasanapalvelun asentaminen onnistui toimeksiantajan tuotantoympäristöön suunnitelmien mukaan. Palvelun asentaminen muusta toimeksiantajan verkosta eriytettynä ei aiheuttanut ongelmia palvelun yhdistämisessä domainiin tai sen käyttöönotossa. Oletin ennalta, että salasanapalvelun yhdistäminen SMS-välityspalvelun kanssa olisi opinnäytetyön vaikein osuus. Yllätyinkin, kuinka selkeä prosessi loppujen lopuksi oli. Tarvittavan http-portin avaaminen salasanapalvelun verkosta välityspalvelulle, http-parametrien asettaminen ja käyttäjätunnuksen luonti välityspalvelulle onnistui palveluiden dokumentoinnin ja toimeksiantajan kollegan konsultoinnilla nopeasti. SSL-sertifikaatin asennus salasanapalvelun

nettikäyttöliittymän salaamiseksi oli työn vaikein osuus. Palvelun dokumentointi oli vajavainen, mikä aiheutti haasteita asennuksessa. Vasta monen tunnin yrittämisen jälkeen löysimme sattumoisin palveluntarjoajan nettisivuilta erillisen ohjeen SSL-sertifikaatin asentamiseen, mitä ei oltu liitetty mihinkään palvelun viralliseen asennusdokumentaatioon.

Opinnäytetyössäni päästiin toimeksiantajan kanssa sovittuihin tavoitteisiin. Palvelu saatiin asennettua onnistuneesti toimeksiantajan tuotantoympäristöön ja tarvittavat palvelut liitettyä siihen kiinni. Koen implementoidun salasanapalvelun olevan luotettava ja turvallinen käyttää. Vastaisuudessa työtä voitaisiin vielä kehittää lisäämällä siihen tarkka ja selkeä dokumentaatio salasanapalvelun käyttöönotosta, minkä avulla asiakasyritysten käyttäjät saadaan helposti ottamaan uusi palvelu käyttöönsä. Seuraava askel työn jatkamisessa olisi pitää asiakkaille käyttöönottokoulutuksia palvelun käytöstä. Tarkkaa taloudellista hyötyä ei pystytä todentamaan, koska toimeksiantajalla ei ole ollut dataa salasanojen nollaamiseen käytetystä työajasta ennen tämän opinnäytetyön tekemistä.

LÄHTEET

Cox, L. Disruption. Julkaistu 16.03.2017. How Reliable is Cloud Computing? Luettu 26.04.2018. https://disruptionhub.com/reliable-cloud-computing/

Cybertrol Engineering. 2018. Cybertrol Engineering has been at the forefront of the industry since data center virtualization entered the industrial IT space. Katsottu 02.05.2018. http://www.cybertrol.com/wp-content/uploads/2016/03/Virtualization_Infographic-2.png

Heino, P. 2010. Pilvipalvelut. 1. painos. Hämeenlinna: Talentum Media Oy ja Petteri Heino.

Joytsana, G. Znetlive Blog. Julkaistu 08.07.2016. What are the pros and cons of cloud computing? Luettu 25.04.2018. https://www.znetlive.com/blog/pros-and-cons-of-cloud-computing/

Järvinen, P. 2012. Arjen tietoturva vinkit ja ratkaisut. 1. painos. Jyväskylä: Docendo.

Pritchett, A. Compare the Cloud. Julkaistu 21.02.2018. 6 Pros and Cons of Cloud Storage for Business. Luettu 26.04.2018. https://www.comparethecloud.net/articles/6-pros-and-cons-of-cloud-storage-for-business/

Rouse, M. Bacon, M. Techtarget. Päivitetty 27.04.2017. Definition: Password. Luettu 03.05.2018. https://searchsecurity.techtarget.com/definition/password

Rouse, M. Cobb, M. Techtarget. Päivitetty 22.12.2016. Definition: Two-factor authentication. Luettu 2.5.2018. https://searchsecurity.techtarget.com/definition/two-factor-authentication

Rouse, M. Haughn, M. Techtarget. Päivitetty 18.12.2014. Definition: User authentication. Luettu 3.5.2018. https://searchsecurity.techtarget.com/definition/user-authentication

Rouse, M. Moore, J. Techtarget. Päivitetty 15.12.2016. Definition: Cloud Services. Luettu 17.5.2018. https://searchitchannel.techtarget.com/definition/cloud-services

Salo, I. 2010. Cloud computing Palvelut verkossa. 1. painos. Jyväskylä: Docendo.

Salo, I. 2012. Hyötyä pilvipalveluista. 1. painos. Jyväskylä: Docendo.

Shameer Amir. 2017. 4 Methods to Bypass two factor Authentication. Katsottu 03.05.2018. https://shahmeeramir.com/4-methods-to-bypass-two-factor-authentication-2b0075d9eb5f

Viestintävirasto. Julkaistu 27.11.2014. Pilvipalveluiden tietoturva organisaatioille. Luettu 12.05.2018. https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Viestintävirasto. Päivitetty 26.03.2015. Verkkojen ja Palvelujen tietoturva. Luettu 12.05.2018. https://www.viestintavirasto.fi/ohjausjavalvonta/tekninentoimivuusjatietoturva/tietoturva.html

Viswanathan, P. Lifewier. Päivitetty 13.11.2017. Cloud Computing and Is it Really All That Beneficial? Luettu 26.04.2018. https://www.lifewire.com/cloud-computing-explained-2373125