Lappeenrannan teknillinen yliopisto
Tuotantotalouden tiedekunta
Tietotekniikan koulutusohjelma

Diplomityö

Simo Karhu

Microsoftin pilvipalvelut pk-yrityksen päätelaite- ja tiedonhallinnassa

Työn tarkastajat:	Professori Jari Porras KTM Päivi Nousiainen
Työn ohjaajat:	Professori Jari Porras KTM Päivi Nousiainen

TIIVISTELMÄ

Lappeenrannan teknillinen yliopisto
Tuotantotalouden tiedekunta
Tietotekniikan koulutusohjelma

Simo Karhu

Microsoftin pilvipalvelut pk-yrityksen päätelaite- ja tiedonhallinnassa

Diplomityö

2014

99 sivua, 29 kuvaa, 10 taulukkoa, 2 liitettä

Työn tarkastajat: Professori Jari Porras, KTM Päivi Nousiainen

Hakusanat: Office 365, Windows Intune, Microsoft Azure, pilvipalvelut, päätelaitehallinta, tiedonhallinta

Diplomityössä tutkittiin Microsoftin pilvipalveluiden käyttöä pk-yrityksen päätelaitteiden hallinnassa sekä yrityksen tiedonhallinnassa. Kohdeyrityksenä oli pk-yritys, jolla on ollut Microsoftin pilvipalveluita käytössä jo useamman vuoden ajan. Pilvipalveluiden nopean päivitystahdin myötä uusimpien ominaisuuksien hyödyntäminen on suurelta osin jäänyt tekemättä. Tutkimus päädyttiin rajaamaan kohdeyrityksessä tehdyn vaatimusmäärittelyn mukaisiin tapauksiin, joihin pyrittiin etsimään vastauksia Microsoftin pilvipalveluiden tämän hetken ominaisuuksien avulla.

Tutkimus toteutettiin tutustumalla kirjallisuuden avulla pilvitoimintamallin perusteisiin ja Microsoftin tarjoamiin pilvipalveluihin. Työn käytännön osuus toteutettiin useilla eri päätelaitteilla Office 365:den ja Windows Intunen muodostamassa testiympäristössä, jota laajennettiin Microsoft Azuren mahdollistamilla lisäominaisuuksilla.

Pilvitoimintamallin yritykset taistelevat jatkuvasti käyttäjien luottamuksesta ja NSA:n vakoilutapauksen jälkeen palveluissa on tapahtunut paljon parannuksia. Tutkimuksessa todettiin erityisesti tiedon suojaamiskäytäntöjen ja hallintaominaisuuksien kehittyneen viime vuosina pilvitoimintamallin yritysten keskinäisen kilpailun myötä. Microsoftin pilvipalvelujen uudet ominaisuudet tarjoavat pk-yritysten käyttöön tehokkaita päätelaite- ja tiedonhallintaratkaisuja, joita on tähän asti ollut saatavilla vain suuryritysympäristöissä.

ABSTRACT

Lappeenranta University of Technology

School of Industrial Engineering and Management

Degree Program in Information Technology

Simo Karhu

Microsoft cloud services in SMEs device and information management

Master's Thesis

2014

99 pages, 29 figures, 10 tables, 2 appendices

Examiners: Professor Jari Porras, M.Sc. Päivi Nousiainen

Keywords: Office 365, Windows Intune, Microsoft Azure, Cloud services, device management, information management

This thesis researched the use of Microsoft's cloud services in device management and information management within SMEs. The case study company featured was a SME which has made use of Microsoft's cloud solutions already for several years. Due to the fast development of these technologies, the full utilization of the recent features has not been fully undertaken. This thesis only included cases which were in accordance to the requirement specifications of the featured company, aiming to solve the cases using the latest features of Microsoft's cloud based services.

The study was undertaken reviewing literature on the basics of cloud technologies and the services offered by Microsoft. The practical part of the thesis was carried out by using various devices in a test environment. Trial versions of Office 365 and Windows Intune were run in the test environment and were further developed by using additional features from Microsoft Azure.

The cloud service providers constantly compete to gain the users' trust. Especially after the much published NSA case, where there after the cloud based technologies saw great improvements. This study discovered that the information security practises and management features have been much improved in recent years due to the competition between cloud providers. Microsoft's new cloud service features offer efficient device and information management solutions for SMEs which until recently have only been available for large enterprises.

Sisällysluettelo

1 Johdanto 1
1.1 Työn tausta 1
1.2 Kohdeyritys 3
1.2.1 Hallinnan nykytilanne 3
1.2.2 Yrityksen tavoitetila 5
1.3 Työn tavoitteet ja rajaukset 6
1.4 Tutkimuksen toteutus 7
1.5 Raportin rakenne 8
2 Pilvitoimintamalli 10
2.1 IT-infrastruktuurin muutos 10
2.2 Pilvitoimintamallin kuvaus 15
2.3 Pilvitoimintamallin tekniikka 21
2.4 Palveluiden turvallisuus 24
2.5 Luottamuksen rakentuminen pilvitoimintamallissa 28
2.6 Pilvipalveluiden käyttöönoton vaikutuksia yrityksen tiedonhallintaan 31
3 Microsoftin pilvipalvelut yrityksille 35
3.1 Microsoft Azure 36
3.2 Office 365 39
3.2.1 Exchange Online 41
3.2.2 SharePoint Online 42
3.2.3 Lync Online 44
3.2.4 OneDrive for Business 44
3.3 Windows Intune 45
3.4 Luottamus Microsoftin pilvitoimintamallissa 47
3.4.1 Pilvipalveluiden sisäänrakennetut turvaominaisuudet 49
3.4.2 Käyttäjän hallinnoimat turvaominaisuudet 51
4 Tutkimuksen toteutus testiympäristön avulla 55
4.1 Tutkimusympäristön laitteet ja ohjelmistot 55
4.2 Microsoftin pilvipalveluiden käyttöönotto 56
4.3 Windows Intune testiympäristössä 58
4.3.1 Windows Intunen Mobile Device Management 60
4.3.2 Asennettujen ohjelmistojen hallinta 64
4.3.3 Etätoimenpiteet tietokoneille 64

4.3.4 Tietoturvan valvonta 65
4.4 Office 365 testiympäristössä 67
4.4.1 Tiedostojen käyttö 68
4.4.2 Sisältöoikeuksien hallinta 71
4.4.3 Monivaiheinen todentamismenettely 77
4.4.4 Mobiililaitteiden hallinta 79
4.4.5 Tietototurva ja yhteysongelmiin varautuminen 81
4.5 Pilvipalveluiden kustannusten arviointi 82
5 Työn tulokset 84
5.1 Työn tulosten arviointi 90
6 Johtopäätökset 93
Lähdeluettelo 95
Liitteet 100

1 JOHDANTO

Tietotyön merkitystä yritysten tuloksellisuuteen ei nykyään kiistetä edes perinteisimmillä teollisuudenaloilla, rakennusala mukaan lukien. Työskentelyn malli on lisäksi muuttunut perinteisestä toimistotyöskentelystä enemmän paikkariippumattomaksi, jossa työt voidaan tehdä päätelaitteella kaikkialta, missä internet-yhteys on käytössä. Tämän työskentelyn vapauden on mahdollistanut mobiiliteknologian voimakas kehitys 3G- ja 4G-tekniikoiden myötä. Tämä toisaalta on johtanut siihen, että työskentelyyn on käytettävissä monia eri päätelaitteita perinteisen tietokoneen lisäksi. Tietotekniikka onkin nykyisin kaikkialla - jopa rakennustyömailla työskentelevät kaivinkonekuskit toimivat valmiiden 3D-mallien avulla ja tarvittaessa tieto saadaan siirrettyä reaaliajassa työnjohdon nähtäväksi tietokoneelle, älypuhelimelle tai tablettitietokoneelle.

1.1 TYÖN TAUSTA

Fyysisesti hajautettu työskentely, joka tapahtuu yrityksen sisäverkon ulkopuolelta, aiheuttaa usein lisätyötä yritysten IT-osastoille. Kun kyseessä ovat pienet ja keskisuuret yritykset tilanne vaikeutuu edelleen, koska usein omaa IT-osastoa ei ole tai sillä ei ole riittävää tietämystä, kuinka työasemien suojaus ja turvalliset yhteydet yrityksen verkkoon tulisi toteuttaa oman toimiston ulkopuolelta. Silloin kun omaa IT-osastoa ei ole palvelinten ylläpitoon, tarvittavat palvelimet ja työasemien hallintapalvelut on jo aiemmin ulkoistettu tai ohjelmistot ostettu suoraan palveluna, pilvipalvelumallin mukaisesti. Varsinkin uudempien pk-yritysten kyseessä ollen vanha IT-infrastruktuuri ei rajoita valintoja, joten tilanne voi olla jopa sellainen, että kaikki yrityksen tarvitsemat ohjelmistot ja palvelut toimivat pilvipalveluina ja perinteinen IT-infrastruktuuri sisältää ainoastaan verkkokytkimet. Näissä tapauksissa yrityksen oman sisäverkon merkitys pienenee ja tärkeäksi ominaisuudeksi muodostuu yksittäisten työasemien ja yritysdatan suojaaminen sekä luotettavien yhteyksien luominen yrityksen käytössä oleviin sovelluksiin.

Yksittäisten työasemien hallinta ja suojaaminen monimutkaistuu, kun käytössä on sekava laite- ja ohjelmistokanta. Tämä onkin monissa pk-yrityksissä alkutilanne,

kun laitteita on ostettu mahdollisesti jo vuosia ilman suurempaa suunnittelua. Kuitenkin pienissäkin yrityksissä tulisi miettiä, miten on mahdollista päästä kohti vakioitua laite- ja ohjelmistokantaa. Tällöin laitteiden koko elinkaari saataisiin hyödynnettyä ja laitteiden aiempaa luotettavampi toimivuus mahdollistaisi myös yrityksen tuloksellisen kasvun.

Ohjelmistojen vakioinnissa auttavat ohjelmistotoimittajien lisensointisopimukset. Monesti nämä ovat pk-yrityksen käyttöön liian kalliita ratkaisuja verrattuna uusien koneiden mukana ostettaviin esiasennettuihin ohjelmistoihin, tai ohjelmistot ovat vain suuyritysten saatavissa. Pilvipalvelut tarjoavat yhden uuden ratkaisun lisensointiongelmaan. Tässä mallissa yritys maksaa ohjelmista vain käytön mukaan ja välttyy täten ylimääräisiltä lisensointimaksuilta sekä ylimääräisiltä laiteinvestoinneilta, joita ohjelmiston hankkiminen yritykselle mahdollisesti aiheuttaisi. Pilvipalvelut mahdollistavat kausiluontoisen työntekijävaihtelun ilman lisäkustannuksia, jotka perinteisessä lisensointimallissa jouduttaisiin maksamaan. Lisäksi käytössä on kaikilla sama ja uusin versio ohjelmistosta.

Microsoft toi vuoden 2011 aikana markkinoille kaksi merkittävää pilvipalvelua, joiden avulla yritykset voivat halutessaan vakioida käyttämänsä käyttöjärjestelmät sekä toimisto-ohjelmistot. Nämä palvelut ovat Office 365 ja Windows Intune.

Office 365 -pilvipalvelu tuo yritykselle useita yhteistyö- ja viestintätyökaluja hyödyntäen suosittuja Microsoft Office toimisto-ohjelmistoja. Office 365 -pilvipalvelusta on tarjolla useita eri versioita kuukausimaksua vastaan. Kuukausimaksua vastaan voi tilata myös version, jossa työasemalle saa asentaa uusimman version Office-ohjelmistosta.

Myös Windows Intune on pilvisovellus, mutta sillä mahdollistetaan työasemien ja mobiililaitteiden hallinta hajautetussa toimintaympäristössä ilman omien hallintapalvelimien perustamista tai tarvetta yrityksen sisäverkolle. Windows Intunen kuukausimaksuun kuuluu lisäksi oikeus käyttää mitä tahansa Windowsin käyttöjärjestelmää työasemassa.

Office 365:den ja Windows Intunen rinnalla markkinoille on tullut myös muita Microsoftin pilvipalveluita, jotka yhdessä käytettynä muuttavat yrityksen perinteistä tapaa toimia. Pilvipalvelut ovat viime vuosina kehittyneet huimaa vauhtia: ohjelmistoista julkaistaan jatkuvasti uusia kehitysversioita ja käyttäjät saavat sitä kautta uusia ominaisuuksia hyödynnettäväkseen. Nämä uudet ominaisuudet jäävät helposti yrityksissä hyödyntämättä ajanpuutteen tai tietämättömyyden takia. Onkin aika tutkia nykytilanne ja selvittää, mitä mahdollisuuksia kyseiset palvelut pk-yrityksille tarjoavat.

1.2 KOHDEYRITYS

Diplomityö tehtiin rakennusalan pk-yritykseen, joka on kasvanut yhden pääkonttorin ympäristöstä useamman toimipisteen yritykseksi. Toimipisteillä työskentelevät henkilöt ovat yrityksessä vähemmistönä: suurin osa työskentelee ympäri Suomen sijaitsevilla työmailla.

1.2.1 HALLINNAN NYKYTILANNE

Yrityksen toiminta on laajentunut ajan kuluessa maanlaajuiseksi, ja työmaat ovat kestoiltaan ja suuruudeltaan hyvin vaihtelevia – lyhimmät työmaat ovat ohitse muutamassa päivässä, kun toiset kestävät useita vuosia. Muuttuvien työmaiden ympärille on ollut kallista ja paikoitellen mahdotonta rakentaa perinteistä yritysverkkoa, johtuen huonoista tietoliikenneyhteyksistä sekä työmaiden nopeasta vaihtuvuudesta.

Yrityksen kasvu on ollut 2000- luvulla nopeaa, ja samanaikaisesti tietotekniikka on tullut myös perinteiselle rakentamisen alalle. Kohdeyrityksellä ei kuitenkaan ole ollut omaa verkkoinfrastruktuuria päätoimipistettä lukuun ottamatta, mikä on johtanut päätelaitteiden hallinnan sekä erityisesti laitteiden sisältämän tiedon säilyttämisen ongelmiin. Ajan kuluessa hankitun sekalaisen ja alati kasvavan laitekannan ylläpito muodostui liian työlääksi. Samanaikaisesti päätelaitteilla sijaitsevien tiedostojen määrä on kasvanut valtavasti.

2000-luvun alusta aina vuoteen 2006 työmaayhteydet luotiin lankapuhelinverkon kautta. Tämä mahdollisti myös vielä tuolloin rakennusalalla laajalti käytössä olleiden fax-laitteiden käytön suoraan puhelinverkon kautta. Vuonna 2006 3G-tekniikka otti suuren harppauksen UMTS (Universal Mobile Telecommunications System) -verkon myötä [1]. 2010-luvulla mobiiliyhteydet ovat nopeutuneet suurin harppauksin ja uusien taajuuksien avulla peittävät nykyisin hyvin jo suurimman osan Suomesta. Tämä on mahdollistanut monin paikoin riittävän nopeat verkkoyhteydet myös työmailta käsin.

Mobiiliyhteyksien tultua yhä käyttökelpoisemmiksi ja yrityksen hajanaisuuden vuoksi yrityksessä otettiin käyttöön Microsoftin Windows Intunen ensimmäinen versio päätelaitteiden hallintaan jo heti sen julkaisun aikoihin vuonna 2011. Intunen pilvipohjaisen hallintakonsolin avulla sekä toimistojen että työmaiden tietokoneet saatiin yhtenäisen hallinnan ja valvonnan piiriin.

Yrityksen sähköpostipalvelin on ollut ulkoistettuna koko sen olemassaolon ajan. Ensimmäinen liikkuvaan työhön tarkoitettu ulkoistettu ratkaisu otettiin käyttöön 2008. Tämän ratkaisun avulla yrityksessä saatiin sähköpostit Mail for Exchange -tekniikan avulla myös joihinkin matkapuhelimiin. Tuon jälkeen muutoksia sähköpostijärjestelmiin on tehty kahteen otteeseen - vuoden 2012 lopulla siirtyminen Microsoftin Office 365:den käyttöön toi näkyvimmät muutokset käytönhallinnan puolelle. Erityisesti matkapuhelimien ja sähköpostilla siirrettävän datan hallintamahdollisuudet paranivat huomattavasti. Käytössä olevat pilvipalveluratkaisut ovat vaikuttaneet soveltuvilta yrityksen käyttöön mutta ovat nykyisin ominaisuuksiltaan niin laajoja, ettei yrityksellä ole ollut resursseja tutkia, kuinka niitä parhaiten hyödynnettäisiin.

Tiedostojenhallintaan yritys käyttää useita eri ratkaisuja; työmaiden tarpeet eroavat melko paljon toimistojen tarpeesta. Yrityksessä käytetään työmaiden tiedostojenhallintaan erinäisiä alalla toimivia projektipankkisovelluksia. Projektipankkien käyttöönotto on johtunut alun perin tilaajien vaatimuksista. Yrityksen intranet toimii Office 365:den mukana tulevan SharePoint Online -palvelun päällä. Intranetin

käyttö on ollut yrityksessä melko vähäistä. Yhteistä intranetsivustoa suositumpia ovat olleet erilaiset työryhmätilat, jonne vain määritetyillä ryhmillä on pääsy. Sähköposti on edelleen tiedonvälityksessä yrityksen tärkein väline.

Yrityksen laitekanta on hankittu vähitellen, joten laitteisto on vielä osin sekalainen. Reilun kolmen vuoden ajan tietokoneita hankittaessa on panostettu saman mallisarjan tuotteisiin, jolloin näiden laitteistotyypit lähestyvät jo toisiaan. Samalla hallittavien ohjelmistojen ja laiteajureiden kirjo on saatu hallintaan. Matkapuhelimien kohdalla vaihtuvuus mallistoissa on tietokoneita nopeampaa, ja yrityksessä on tapahtunut viimeisen vuoden aikana nopeaa siirtymistä kohti älypuhelimia. Näiden hankinnassa on päädytty käyttämään muutamaa poikkeusta lukuun ottamatta Windows Phone -tuotteita.

Yrityksellä ei ole ollut yhtä yhteistä lisenssisopimusta toimisto-ohjelmistoihin, vaan ohjelmistot ovat hankittu erillisinä ohjelmistoina laitteiden hankinnan yhteydessä. Tämä on johtanut IT-tuen antamisen ongelmiin, kun eri versiot ohjelmista toimivat aina hieman eri tavalla. Yrityksellä on ollut sekaisin käytössä Microsoft Officen versioita 2007, 2010 ja 2013. Uusimmat 2013 versiot on otettu käyttöön Office 365:den kautta kuukausimaksullisina versioina, jolloin näiden ohjelmistojen versiot pysyvät aina ajan tasalla. Versioiden yhteen saattamisen vuoksi kaikki uusien tietokoneiden käyttöjärjestelmät ja toimisto-ohjelmistot tulevat nykyisin pilvipalveluiden lisenssien kautta.

1.2.2 YRITYKSEN TAVOITETILA

Yrityksellä on jo nykyisin käytössä hyvät ja ajantasaiset välineet hallinnan toteuttamiselle. Suurin ongelma tällä hetkellä on eri palveluiden hajanaisuus ja osin päällekkäisyys. Muun muassa Office 365 ja Windows Intune eivät yrityksessä toimi samoilla tunnuksilla, joten kaikkia ohjelmistojen mahdollistamia hyötyjä ei yrityksessä tällä hetkellä saada käyttöön. Tavoitetilassa kaikki yrityksen järjestelmät toimivat yhden tunnuksen kautta - niin hallinnan kuin myös käyttäjien osalta. Ohjelmistojen jakelu saadaan tarvittaessa suoritettua laitealustasta riippumatta.

Yrityksen datanhallinnan tavoitetilassa käyttäjät eivät enää työstä jatkuvasti uusia erillisiä tiedostoja, vaan jo olemassa olevia tiedostoja käytetään hyödyksi dokumenttienhallintaratkaisun avulla. Yrityksen asiakirjoissa käytetään yhtenäisiä dokumenttipohjia läpi organisaation. Lisäksi dokumenttienhallinta pohjautuu tarkoituksenmukaiseen metarakenteeseen. Yrityksen datan suojaus tulee toteuttaa siten, ettei kriittistä tietoa jaeta yrityksen ulkopuolelle tahallisesti eikä tahattomasti.

1.3 TYÖN TAVOITTEET JA RAJAUKSET

Office 365 ja Windows Intune ovat erittäin laajoja tuotekokonaisuuksia, joita yhdessä diplomityössä ei voida kokonaan käsitellä. Molemmat ohjelmistot ovat olleet kohdeyrityksen käytössä lähes niiden koko elinkaaren ajan, mutta ajan myötä tulleita uusia ominaisuuksia yrityksessä ei ole täysin hyödynnetty. Tämän diplomityön tavoitteen ja rajauksien asettelun lähtökohtana toimii yrityksessä tehty vaatimusmäärittely, jolla yrityksessä päästäisiin kohti haluttua tavoitetilaa. Vaatimusmäärittelyn pohjalta työssä käsitellään, kuinka yrityksessä on toimittu tähän asti, ja tutkitaan, voivatko ohjelmistojen uudet ominaisuudet tehostaa toimintaa ja parantaa yrityksen tietoturvaa.

Diplomityössä keskitytään tilanteeseen, jossa toimitaan kokonaan pilviympäristössä. Windows Intunen kohdalla työssä ei oteta laajemmin kantaa perinteisiin päätelaitteiden hallintametodeihin ja vertailla kilpailijoiden tuotteita keskenään. Samoin Office 365:den kohdalla työssä ei tehdä vertailua muihin vastaaviin palveluihin, eikä tutkita sen sisältämien palveluiden toteutusta omien palvelinten avulla.

Työn toteutusvaiheessa pyritään myös selvittämään eri mobiililaitteiden soveltuvuutta Microsoftin pilvipalveluiden käyttöön niin laitehallinnan kuin myös tiedonhallinnan näkökulmasta. Niiden mobiililaitteiden osalta, joita ei ole mahdollisuutta saada testiin, tutkimus tehdään löytyvän dokumentaation perusteella.

Tiedonhallintaa tutkittaessa työssä ei ole tarkoitus paneutua Office 365:den mahdollistamaan dokumenttienhallinnan toteutukseen vaan keskittyä siihen, kuinka yrityksen järjestelmissä oleva kriittinen tieto saadaan kyseisillä palveluilla säilytettyä yrityksen hallinnassa ja vain tietoa tarvitsevien käytössä.

1.4 TUTKIMUKSEN TOTEUTUS

Diplomityön tutkimusongelmana on selvittää Microsoftin pilvipalveluiden nykytilan soveltuvuus pk-yrityksen päätelaitteiden hallintaan ja tiedonhallintaan toimittaessa hajautetussa ympäristössä useilla eri päätelaitteilla.

Työn alkuvaiheessa yrityksen IT-henkilöstö teki yhdessä yrityksen johdon kanssa vaatimusmäärittelyn pilvipohjaisten toimisto- ja hallintasovellusten käyttötilanteista, joihin käytössä olevien palveluiden avulla haluttaisiin saada vastaus. Vaatimukset numeroitiin tärkeyden mukaisesti yhdestä kolmeen - numero yhden tarkoittaessa tärkeintä vaatimusta. Nämä 17 yrityksessä määriteltyä tilannetta ovat (vaatimuksen tärkeys yritykselle on esitetty suluissa):

- *Kaikkien yritysten tietokoneiden hallinta riippumatta sijainnista (1)*
- *Tiedot asennetuista ohjelmistoista ja niiden versioista (2)*
- *Lisenssien hallinta järjestelmän avulla (2)*
- *Mobiililaitteiden hallinta (1)*
- *Käyttäjän tiedostot käytettävissä kaikilla päätelaitteilla (2)*
- *Yrityksen yhteiset tiedostot saavutettavissa kaikilla päätelaitteilla (2)*
- *Tietoturvan valvonta ja määritykset (1)*
- *Etätoimet laitteille esimerkiksi katoamistapauksessa (1)*
- *Tiedon suojaaminen koneen kovalevyllä (1)*
- *Käyttäjätuki etäyhteyden avulla (3)*
- *Ohjelmistojen asennukset ja päivitykset (2)*
- *Yrityksen datan suojaaminen (1)*
- *Projektien tiedostojen jako ja arkistointi (3)*
- *Yhdet kirjautumistunnukset (2)*
- *Turvallinen sähköpostiliikenne (1)*

- *Käyttäjän salasanan hyödyntämisen havaitseminen (2)*
- *Yhteysongelmatilanteissa toiminnan jatkuminen (1)*

Tämän diplomityön tutkimusotteena on tapaustutkimus. Työn toteutus jakautuu kirjalliseen osioon sekä soveltavan koeympäristön luomiseen, jossa testataan pilvipalvelujen ominaisuuksia eri alustoilla. Koeympäristön tutkimustilanteiden jaottelu tehtiin yhdistelemällä yrityksen vaatimusmäärittelyn käyttötilanteet Windows Intunen ja Office 365:den kesken. Vaatimusmäärittelyn ja yrityksen tavoitetilan pohjalta luotiin tutkimuskysymykset, joihin etsittiin vastauksia teoriaosuuden ja koeympäristön kautta.

Päätutkimuskysymyksenä on:

- Miten tutkittujen pilvipalveluiden uudet ominaisuudet voisivat parantaa kohdeyrityksen päätelaite- ja tiedonhallintaa?

Tarkentavat alakysymykset:

- Mitä mahdollisuuksia palvelut tuovat yrityksen kriittisen datan suojaamiseksi?
- Kuinka eri mobiilipäätelaitteet toimivat yhdessä palvelujen kanssa?
- Miten palvelujen saavutettavuus ja jatkuvuus on turvattu?
- Kuinka turvallisina palveluita voidaan pitää verrattuna oman palvelinsalin ratkaisuihin?

1.5 RAPORTIN RAKENNE

Ensimmäisessä luvussa käsitellään työn taustaa ja kohdeyrityksen tiedonhallinnan nykytilaa ja tavoitetta. Lisäksi määritellään tutkimuksen tavoitteet ja rajaukset sekä määritellään tutkimuksen toteutusmenetelmä.

Toisessa luvussa käsitellään IT-infrastruktuurin muutosta perinteisistä yrityskohtaisista oman palvelinsalin ratkaisuista kohti pilvitoimintamallia ja lisäksi sitä, mitä muutoksia pilvitoimintamallin käyttöönotto yrityksessä aiheuttaa. Luvussa käydään läpi eri pilvipalvelumallien eroja ja tarkastellaan, mitä vaikutuksia palvelumallin

valinnalla on palveluiden hallintaan ja uhkakuviin. Lisäksi luvussa käsitellään luottamuksen rakentumiseen vaikuttavia tekijöitä.

Luvussa 3 käydään läpi Microsoftin tarjoamia pilvipalveluita yrityksille sekä niiden ominaisuuksia. Luvussa käsitellään myös, kuinka Microsoft pyrkii rakentamaan luottamusta palveluihinsa sisäänrakennettujen turvaominaisuuksien keinoin.

Luvussa 4 toteutetaan tutkimusympäristö, jossa testataan Microsoftin pilvipalveluiden toimivuutta kohdeyrityksen omaisessa ympäristössä. Tutkimusympäristössä keskitytään kohdeyrityksen vaatimusmäärittelyn mukaisiin tilanteisiin, joihin vastausta haetaan luvussa 3 esiteltyjen turvaominaisuuksien kautta.

Luvussa 5 esitetään työn tulokset vastaamalla luvussa 1 esitettyihin tutkimuskysymyksiin. Lisäksi luvussa arvioidaan saatujen tulosten merkitystä tutkimuksen ja yrityksen kannalta.

Luku 6 on koko työn yhteenvetokappale, jossa koostetaan tiivistetysti yhteen työn keskeisin sisältö.

2 PILVITOIMINTAMALLI

Tietotekniikan kuluttajaistuminen aiheuttaa nykypäivänä yrityksille uusia haasteita. Käyttäjät ovat tottuneet kuluttajapuolen sovelluksien kautta pääsemään käsiksi tarvitsemiinsa tietoihin päätelaitteesta ja sijainnista välittämättä. Samat vaatimukset ovat tulleet vauhdilla käyttäjien mukana yritysympäristöön ja tuoneet samalla paljon lisähaasteita yrityksen IT-infrastruktuurille (kuva 1). Käyttäjät olettavat tavoittavansa työresurssinsa kaikkialta useilla eri päätelaitteilla. Kasvanut laite- ja sovelluskanta monimutkaistaa päätelaitehallintaa ja luo samalla uusia ongelmia yrityksen datan suojaamiseen. [2]

Kuva 1. Nykyajan IT-infrastruktuurin haasteet syntyvät moninaisesta laite- ja sovelluskannasta. [2]

Perinteisellä palvelinkeskeisellä Client-Server -infrastruktuurilla nykyaikaisen IT-ympäristön hallinta muodostuu nopeasti liian raskaaksi ja erittäin kalliiksi. Tämän takia palvelinten toteutuksessa kehitys on mennyt kohti käyttäjä- ja palvelukeskeistä IT-infraa.

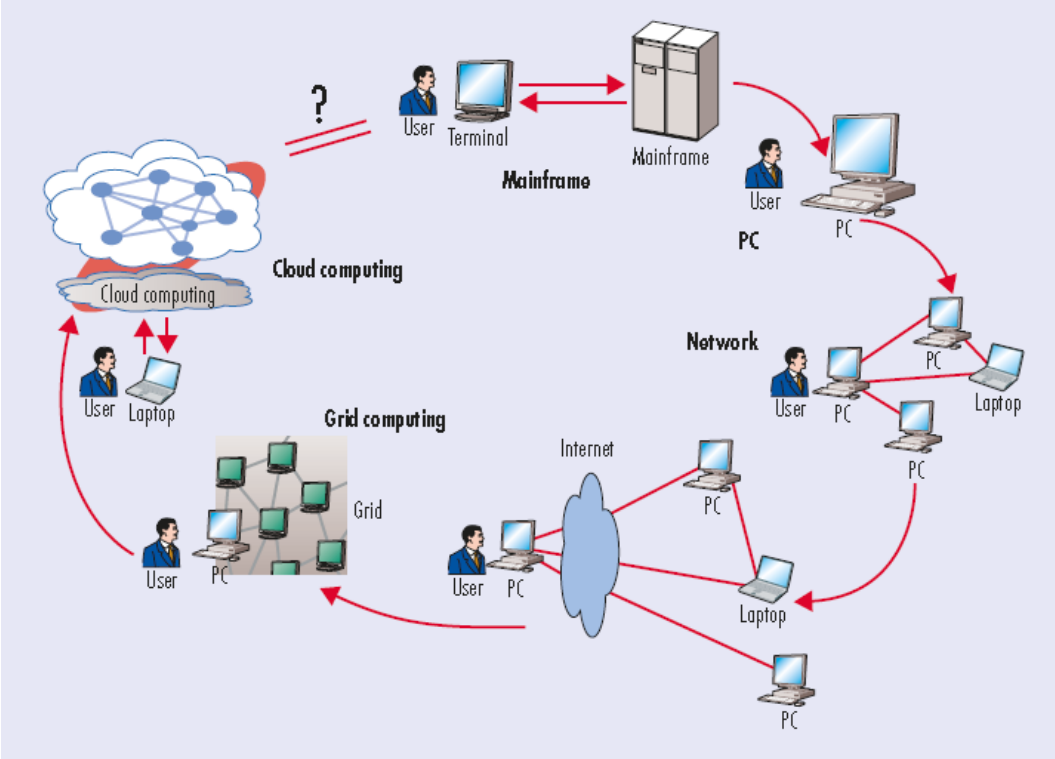
2.1 IT-INFRASTRUKTUURIN MUUTOS

Tietokoneen käytön ajatusmalli on muuttunut useaan otteeseen vuosien saatossa, ja nämä muutokset on eriteltävissä kuuteen eri vaiheeseen (kuva 2). Ensimmäisessä

vaiheessa oli keskuskonetoimintamalli (kuvassa 2, mainframe), jossa käyttäjä otti terminaalipäätelaitteen avulla yhteyden keskuskoneeseen, jossa kaikki laskentaa tarvitsevat toimet suoritettiin. Jo tuolloin oli käytössä virtualisointiajattelu, jossa päätteille jaettiin keskuskoneelta virtualisoitu kapasiteetti ja kaikki laskenta tapahtui keskuskoneen resursseilla. Virtualisointi kuitenkin hävisi 1990-luvulla x86-pohjaisten tietokoneiden myötä, ja tuki x86-alustan virtualisoinnille tuli vasta vuonna 2005 [3] .

Keskuskoneiden jälkeen siirryttiin henkilökohtaisten tietokoneiden (kuvassa 2, PC) käyttöön. Tietokoneiden teho alkoi riittää tarvittavan laskentatehon takaamiseksi ja koneen laskentatehoa ei tarvinnut jakaa kenenkään muun kanssa. Kolmannessa vaiheessa tulivat tietoverkot (kuvassa 2, network), joissa useat tietokoneet muodostivat keskenään paikallisen verkon, jossa voitiin jakaa keskenään samoja resursseja – esimerkiksi tiedostoja ja tulostimia. [4]

Internet-verkon muodostuminen käynnisti neljännen vaiheen, ja se mahdollisti globaalit tietoverkot ja etäohjelmistojen ja resurssien käytön. Viidennessä vaiheessa alkoi herätä ajatus sähköverkon tapaisesta palveluverkosta (kuvassa 2, grid computing), jossa ikään kuin sähköverkon lailla pistokkeesta olisi saatavilla laskentatehoa ja tallennustilaa hajautetun laskennan kautta. Tässä ajatusmallissa henkilökohtaiset tietokoneet liitettiin osaksi hajautettua laiteverkkoa, jossa laskentateho jaettiin usean koneen kesken. Viimeisessä kuudennessa vaiheessa (kuvassa 2, cloud computing) on osin palattu takaisin keskuskoneajatteluun ja erityisesti konesalin virtualisointitekniikoihin. Pilvitoimintamalli mahdollistaa helposti skaalautuvan mallin vapaiden resurssien valjastamiseksi Internetin avulla. [4]



Kuva 2. Tietojenkäsittelyn ajatusmallin muuttuminen ajan saatossa. [4]

Tällä hetkellä meneillään oleva vaihe on vahvasti pilvitoimintamalliin nojaava. Perinteisten henkilökohtaisten tietokoneiden määrä tietojärjestelmien käytössä on viimeisien vuosien aikana pienentynyt selvästi. Gartnerin toimitusjohtaja Phil Redman on jo ehtinyt julistaa 1990-luvulta alkaneen PC-tietokoneiden aikakauden päättyneeksi. Älypuhelinten ja tablettien kasvava suosio on johtanut verkkoliikenteen ja samalla myös yritysdatan siirtymiseen mobiililaitteiden piiriin. Samalla yritysdata pirstaloituu yhä useammalle laitteelle. Gartnerin lehdistötiedotteen mukaan vuoteen 2017 mennessä 90 prosentilla yrityksistä on kaksi tai useampia mobiilikäyttöjärjestelmiä käytössään. Tämän vuoksi mobiililaitteiden hallinta tulee entistä tärkeämmäksi, ja tiedotteen mukaan vuonna 2017 65 %:a yrityksistä on ottanut käyttöön jonkin mobiililaitteiden hallintajärjestelmän (Mobile device management, MDM). [5]

Mobiililaitteiden hallinnan lisäksi yrityksille haasteita aiheuttaa moninaisen laitekannan lisensointi. Gartnerin vuoden 2013 raportin mukaan tyypillinen tietotyöläinen käyttää viikossa yrityksensä toimistojärjestelmiä neljän eri päätelaitteen kautta.

Laitteiden ja käyttäjien määrän pohtiminen onkin erityisen tärkeää laskettaessa lisensointikustannuksia. Yrityksen monet sovellukset vaativat lisenssin jokaista laitetta kohden, kun taas pilvipohjaiset palvelut ovat yleisesti käyttäjäkohtaisia sisältäen useamman päätelaitteen käyttölisenssin. Pilvipalveluna tarjottaviin toimistosovelluksiin siirtyminen voikin useissa tapauksissa tuoda yritykselle suuret säästöt. [6]

Pilvipohjaisiin toimistosovelluksiin siirtymisen innokkuus vaihtelee paljon yritysten välillä. Tähän vaikuttaa muun muassa yrityksen koko, toimiala, toiminnan maantieteellinen hajanaisuus sekä muut erityisvaatimukset. Gartnerin arvion mukaan vuonna 2013 pilvipohjaisia toimistosovelluksia käytti yhteensä 50 miljoonaa käyttäjää, mikä on kahdeksan prosenttia kaikista toimistosovelluksia käyttävistä yrityskäyttäjistä. Ennusteen mukaan suurempi siirtymä kohti pilvipalveluita alkaa vuoden 2015 ensimmäisellä puoliskolla. Vuonna 2017 käyttäjiä on 33 % ja vuonna 2022 jo 60 %, mikä on käyttäjämäärissä mitattuna 695 miljoonaa käyttäjää. [6]

Mobiiliteknologian viime vuosien vahva kasvu on lisännyt vaatimuksia yritysten palvelinsalien tekniikoita kohtaan. Pilvipalveluiden avulla pienyrityksilläkin on mahdollisuus päästä hyödyntämään ennen vain suuryritysten käytössä olleita tekniikoita. Boston Colsulting Groupin tekemässä tutkimuksessa havaittiin että uuden tekniikan käyttöönottoon panostavien pk-yritysten liikevaihto kasvoi kolmessa vuodessa jopa 15 % nopeammin kuin muiden vastaavien yritysten. Liikevaihdon kasvun lisäksi tutkimuksessa havaittiin myös selkeää kasvua uusien työpaikkojen syntymisen määrässä. [7]

Pilvipalvelut ovat olleet viimeiset viisi vuotta IT-alan suurin trendi. Pilvipalvelut ovatkin tulleet lähes kaikkien tietoisuuteen älypuhelimien varmistuksien ja sovellusten yhteiskäytön kautta. Tästä huolimatta yritysten siirtyminen näiden palveluiden käyttäjäksi ei ole ollut niin vauhdikasta kuin siitä käytyjen keskustelujen määrästä voisi päätellä. Suurin syy palveluiden piiriin siirtymisen hitaudelle on pilvi-

palveluiden turvallisuuden epäily; yritykset ovat tottuneet pitämään laitteiden ja datan hallinnan itsellään. Pilvimallissa yrityksen tulee luottaa palveluntarjoajan lupauksiin datan ja järjestelmien turvallisuudesta.

Kuitenkin pilvipalveluiden lupaukset yrityksille tulevista hyödyistä ovat liian suuret, jotta ne voisivat jättää asian kokonaan huomioimatta. Pilvimallin tarjoajat ovat kuitenkin törmänneet suureen ongelmaan rakentaessaan luottamusta palveluihinsa. Kyse ei ole pelkästään luottamuksesta itse pilvipalveluja tuottavaan yritykseen, vaan enemmänkin luottamuksesta pilvitoimintamalliin. Epäilyt johtuvat paljolti järjestelmien läpinäkyvyyden puutteesta, kontrollin menettämisestä dataan sekä epäilyksistä tietoturvan vahvuuteen. [8]

Ongelmat juontavat pilvipalveluiden alkuvaiheisiin, jolloin käyttöönotto alkoi ennen kuin asianmukaiset tekniikat onnistuivat häivyttämään luottamukseen liittyvät ongelmat. Uusien pilvipalveluiden ja niiden käyttöönoton välille syntyi luottamuspula, jota yritykset pyrkivät edelleenkin ratkaisemaan. Vaikka pilvitoimintamallin mukaisilla yrityksillä on käytössä perinteiset palvelutasosopimukset, tulisi pilvipalveluissa keskittyä enemmän mahdollisten vahinkojen estämiseen ennakkoon. Mikään palvelutasosopimus ei pysty korvaamaan yritykselle mahdollisesti menetettyä tärkeää dataa tai mainetta. [8]

Pilvitoimintamalliin siirtymisessä on eroteltavissa selkeästi vahvuudet, heikkoudet, mahdollisuudet ja uhkakuvat (taulukko 1). Yrityksen tuleekin pohtia palveluiden soveltumista juuri heidän toimialalleen ja punnita siirtymisestä saatavien hyötyjen määrää.

Taulukko 1. Pilvipalveluiden vahvuuksien, heikkouksien, mahdollisuuksien ja uhkakuvien tarkastelu SWOT-analyysin avulla. [9]

Vahvuudet	Heikkoudet
- Mahdollistaa myös pienempien yritysten osallistua suurta laskentatehoa vaativien palveluiden piiriin - Lähes välitön pääsy laitteistoresursseihin ilman suuria alkukustannuksia - Mahdollistaa uusien innovaatioiden synnyn - Dynaaminen resurssien skaalaus osin mahdollista - Uudenlaisten sovellusten mahdollistaminen - Säästöjä oikeinmitoitetun infrastruktuurin avulla - Virtualisoitujen palvelujen ylläpitokustannukset perinteisiä palveluita alhaisemmat - Käyttäjät pääsevät käyttämään palveluita useiden päätelaitteiden avulla	- Data sijaitsee yrityksen tilojen ulkopuolella - Datan fyysisen sijainnin varmistaminen hankalaa - Palveluiden SLA-tasot eivät välttämättä ole riittäviä suuryritysten kriittisille toiminnoille, vaikka todellisuudessa ylittäisivätkin talon sisäisen tason
Mahdollisuudet	**Uhkakuvat**
- Myös kehittyvät maat pääsevät helpommin käsiksi uusiin teknologioihin ja voivat sitä kautta tehostaa toimintojaan - Useiden eri tietolähteiden tiedoista mahdollisesti muodostuvat uudet palvelut - Yrityksen hiilijalanjäljen pienentäminen	- Yritysten IT-säädökset estävät joidenkin yritysten liittymisen pilvipalveluiden piiriin - Palveluntarjoajan konkurssi - Palvelujen tietoturva - Standardit puuttuvat - Mahdollinen lukkiutuminen palveluntuottajaan - Paikalliset lait vaihtelevat

2.2 PILVITOIMINTAMALLIN KUVAUS

Pilvitoimintamalli (Cloud Computing) kuvaa toimintaa, jossa tietoverkon ylitse tarjotaan, hankitaan ja toteutetaan pilvipalveluita (Cloud Service). Itse termi cloud computing tulee alun perin puhelin- ja tietoliikenneverkkojen parista, joissa on ollut tapana kuvata verkot yksinkertaistuksen vuoksi pilvisymbolilla. [10]

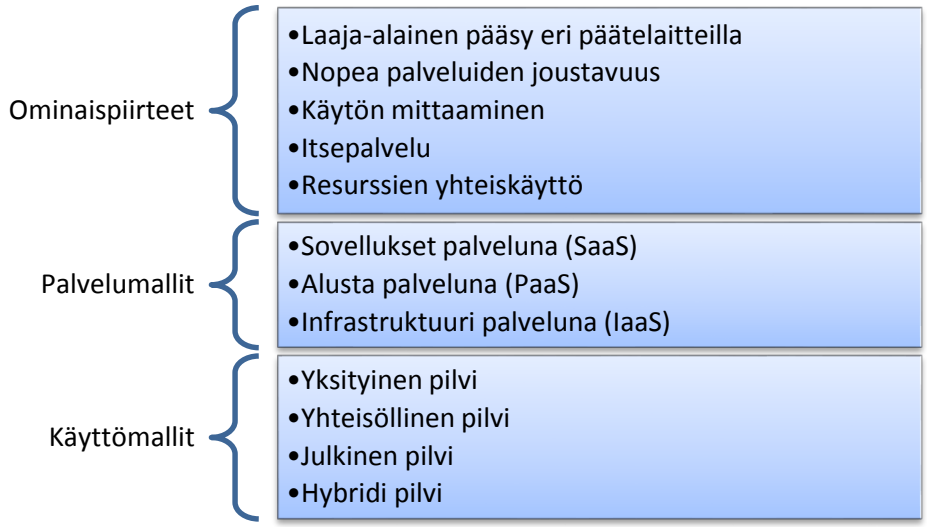
Pilvipalvelu on suomen kieleen vakiintunut termi, jolla yleisesti tarkoitetaan verkosta hankittavia lisäresursseja. Cloud Computing -termistä käytetään myös suomennosta pilvilaskenta. Molempia termejä käytetään kuitenkin sekaisin puhuttaessa pilvi-infrastruktuurin tarjonnasta.

Armbrust et. al. (2010) kuvaa pilvitoimintamallin terminä, joka käsittää niin Internetin välityksellä jaettavat sovellukset kuin myös näiden tarjoamisen mahdollistavan palvelininfrastruktuurin ohjelmistoineen. Pilven ylitse tarjottavista palveluista puhuttaessa tarkoitetaan yleisimmin ohjelmistojen tarjoamista palveluna (Software as a Service – SaaS). Artikkelissaan Armbrust et. al. esittävät myös pilvipalvelutermit infrastruktuurin (IaaS - Infrastructure as a Service) ja alustan tarjoamiseen palveluna (PaaS - Platform as a Service). Tutkimuksen tekemisen aikaan vuonna 2010 hyväksytyt määritelmät vaihtelivat paljon ja ero alemman hierarkiatason infrastruktuurin sekä tätä ylemmän tason alustan tarjoamisen välillä oli hiuksenhieno, joten he käsittelivät IaaS- ja PaaS-malleja yhtenä pilvitoimintamallin tasona. [11]

Nykyisin yksi yleisimmin käytössä oleva määritelmä jakaa IaaS- ja PaaS-mallit omille tasoilleen. Tämä pilvipalveluiden määritelmä on National Institute of Standards and Technology (NIST) julkaisu: “The NIST Definition of Cloud Computing”.

> *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.* [12]

Vapaasti suomennettuna määritelmä kuuluu: Pilvipalvelu on toimintamalli, joka mahdollistaa pääsyn konfiguroitaviin, jatkuvasti verkossa oleviin ja nopeasti skaalautuviin tietotekniikkaresursseihin. Palvelut voidaan ottaa käyttöön hyvin pienillä hallintatoimilla tai palvelun tarjoajan väliintulolla. NIST jakaa pilvipalveluiden määrittelyn viiteen ominaispiirteeseen, kolmeen eri palvelumalliin ja neljään eri käyttöönottotapaan (kuva 3).



Kuva 3. Pilvipalveluiden jaottelu NIST-määritelmän mukaisesti ominaispiirteiden, palvelumallien ja käyttömallien avulla.

Tämän jaottelun mukaiset ominaispiirteet tarkoittavat seuraavaa:

- Laaja-alainen pääsy eri päätelaitteilla: Palvelu tarjotaan esimerkiksi internetselaimen välityksellä, ja se ei ota kantaa päätelaitteeseen.
- Nopea palveluiden joustavuus: Tarvittavien resurssien tulee joustaa niin ylös kuin alas muuttuvan kuorman mukaan.
- Käytön mittaaminen: Palveluista maksetaan käytön mukaan.
- Itsepalvelu: Palvelut tulee pystyä käynnistämään käyttäjän toimesta.
- Resurssien yhteiskäyttö: Samat resurssit ovat usean yrityksen tai käyttäjän käytössä, jolloin ne saadaan tehokkaampaan käyttöön.

[12]

Palvelumallit ylimmältä tasolta alimmalle:

Software as a Service (SaaS) – Sovellukset palveluna

Sovellukset palveluna –malli tarjoaa kuluttajalle palveluntuottajan tarjoaman kapasiteetin päälle toteutetut sovellukset palveluna. Sovellukset ovat käytettävissä useilla eri päätelaitteilla internetselaimen kautta tai erillisen ohjelman käyttöliitty-

män avulla (esimerkiksi Webmail internetselaimen kautta ja Outlook-työpöytäohjelma). Käyttäjä ei yleisesti pääse käsiksi palvelun alla olevaan teknologiaan, vaan hallinta rajoittuu käyttäjäkohtaisten asetusten määritykseen. [12, 11]

Ensimmäisiä SaaS-palveluita hyödyntävä yritys oli SalesForce. Muita tunnettuja SaaS-palveluita ovat muun muassa Zoho, Google Docs ja Microsoftin Office 365. [13]

Platform as a Service (PaaS) – Sovellusalusta palveluna

Palveluntarjoajan luoma sovellusalusta, jolla asiakas voi julkaista omia sovelluksiaan. Asiakas ei pääse käsiksi alustan alapuolella olevaan infrastruktuuriin, mutta hallitsee julkaisemiaan sovelluksia. Joissakin tapauksissa asiakas voi muuttaa joitakin julkaisualustan asetuksia. [12, 11]

Tunnetuimpia palveluntarjoajia ovat Microsoft Azure, Google Apps, BitBucket ja Heroku. [13]

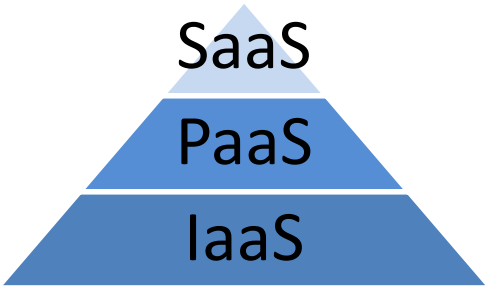
Infrastructure as a Service (IaaS) – Infrastruktuuri palveluna

Asiakas vuokraa käyttöönsä palveluntarjoajan konesalista virtualisoidun palvelintilan, jonka avulla hän voi rakentaa haluamansa infrastruktuurin. Asiakkaan hallinnassa on koko virtuaalialustan päällinen osa. [12, 11]

IaaS-mallin mukaisia infrastruktuurin tarjoajia ovat muun muassa Amazon, Google ja Microsoft.

Palvelumallien jako kolmeen eri tasoon on yleisimmin käytössä oleva määritelmä. Lisäksi on kuitenkin lukematon määrä muita palvelumalleja, joista nykyään käytetään yleisesti nimitystä Everything (tai Anything) as a Service (XaaS) – mitä tahansa -palveluna.

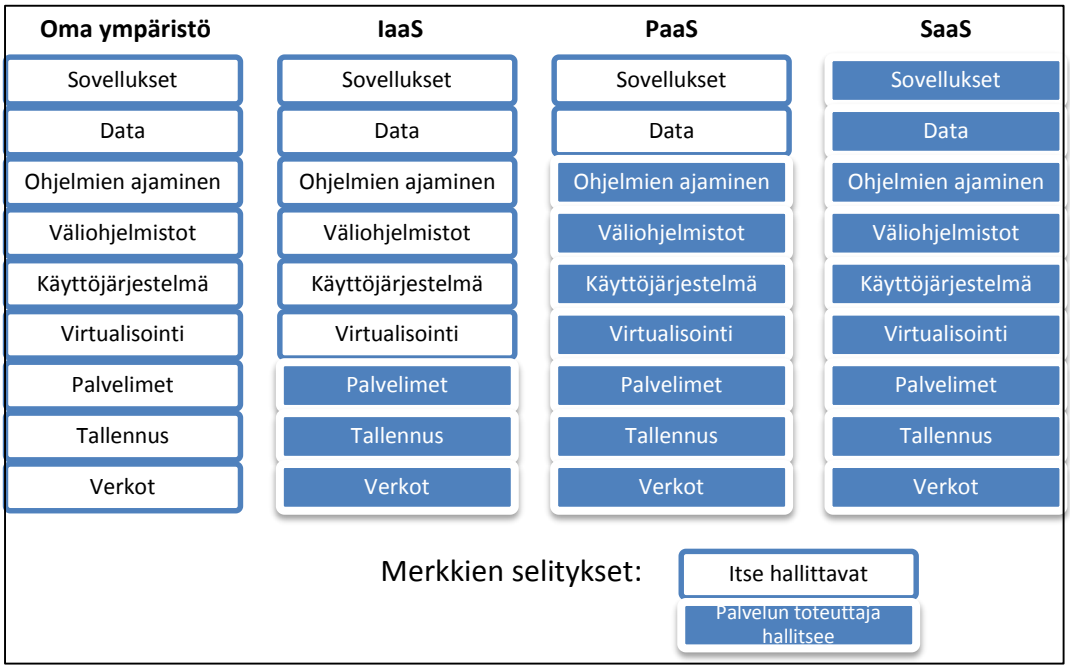
Mell & Grancen (2011) kuvaamat kolme palvelumallia voidaan esittää myös niiden toimintatasojen mukaisesti kerrosmallina, jossa tason leveys kuvaa käsiteltävien sovellusten määrää (kuva 4).



Kuva 4. Pilvipalvelujen palvelumallit kuvattuna toimintatasojen mukaisesti kerrosmallina. [14]

Jos kuvaa 4 ajatellaan pilvipalveluntarjoajien määrän mukaan, pyramidi tulisi piirtää ylösalaisin, siten että SaaS taso olisi ylimpänä kaikista leveimpänä. SaaS-sovellusten tarjoajia, ja siten myös käyttäjiä, on moninkertaisesti verrattuna IaaS-tarjontaan. IaaS voidaankin ajatella järjestelmänsuunnittelijoiden tasoksi, PaaS sovellustenkehittäjien tasoksi ja SaaS käyttäjätasoksi. [14]

Palvelutasojen erilaisuus tulee esille, kun otetaan vertailukohdaksi oman konesalin ratkaisu. IaaS-, PaaS- ja SaaS-palvelujen yksi konkreettinen ero ylläpitäjän näkökulmasta on hallintavastuut. Kuvassa 5 on esitetty eri julkaisumallien hallintavastuiden erot oman konesalin ratkaisuun verrattuna. [15]



Kuva 5. Infrastruktuurin hallintavastuut siirtyvät palveluntuottajalle siirryttäessä omasta konesalista kohti sovellusten vuokrausta. [15]

Pilvipalvelujen käyttömallit:

Private cloud – yksityinen pilvi

Pilviarkkitehtuuri on luotu pelkästään yhtä yritystä varten. Sen omistus ja hallinta voivat olla yrityksen itsensä hallinnassa, ulkoistettu kolmannelle osapuolelle tai kummankin hallinnassa. Yksityinen pilvi voi myös sijaita sekä yrityksen tiloissa että niiden ulkopuolella. [12, 11]

Community cloud – yhteisöllinen pilvi

Pilvimallissa useat eri järjestöt jakavat infrastruktuurin keskenään. Järjestöillä on jokin yhteinen intressi, jonka takia kyseinen pilvimalli muodostetaan. Näitä voivat olla esimerkiksi tietoturvan sanelemat ehdot, säädökset, tehtäväsidonnaiset asiat sekä määräystenmukaisuuden valvonta. Yhteisöllisen pilven omistus ja hallinta voivat olla yhden tai useamman yhteisössä mukana olevan yrityksen hallinnassa, ulkoistettu kolmannelle osapuolelle tai sekä että/kummankin hallinnassa. Yhteisöllinen pilvi voi myös sijaita sekä yrityksen tiloissa että niiden ulkopuolella. [12, 11]

Public cloud – julkinen pilvi

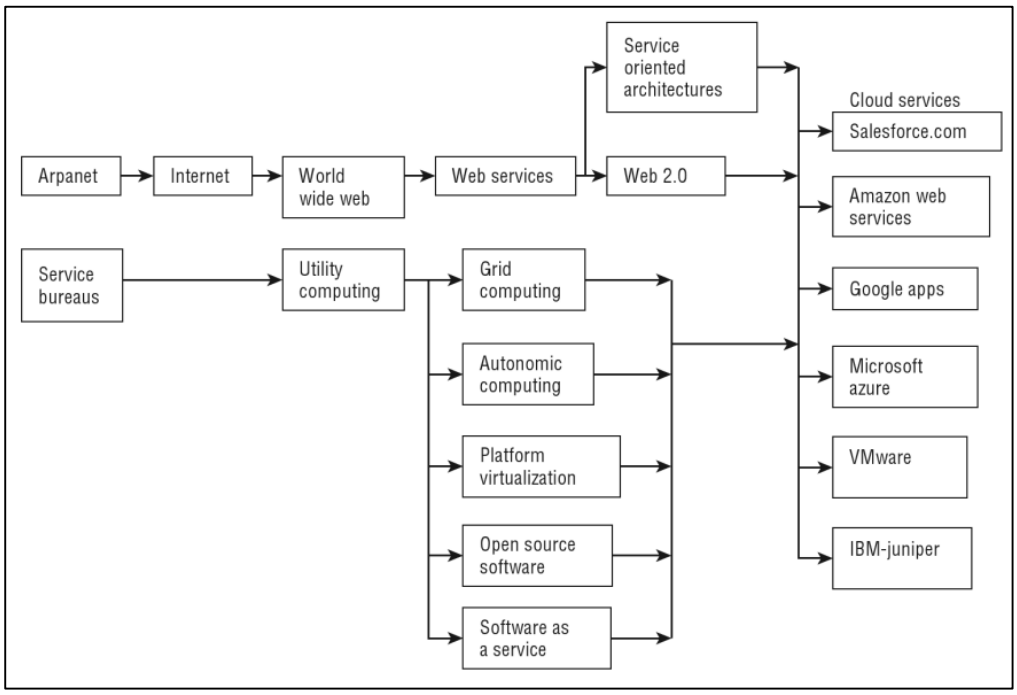
Pilviarkkitehtuuri on avoimessa julkisessa käytössä. Sen omistus, hallinnointi ja operointi tapahtuvat joko kaupallisen yrityksen, akateemisen ympäristön tai julkishallinnon sekä näiden eri yhdistelmien kautta. Julkinen pilvi sijaitsee pilvipalvelun tarjoajan tiloissa. [12, 11]

Hybrid cloud – hybridi pilvi

Pilvipalveluympäristö muodostuu yhden tai useamman infrastruktuurin yhdistelmänä, jotka säilyvät omina yksikköinään, mutta ovat yhdistetty standardoitujen teknologioiden avulla. Tämä mahdollistaa datan ja sovellusten siirreltävyyden. [12, 11]

2.3 PILVITOIMINTAMALLIN TEKNIIKKA

Pilvipalveluista on alettu puhua vuodesta 2006 lähtien [13]. Pilvipalveluiden käyttöönoton mahdollisti jo olemassa olevien tekniikoiden yhdisteleminen tukemaan pilviarkkitehtuuria (kuva 6) [16].



Kuva 6. Pilvipalveluita edeltäneet tekniikat yhdessä mahdollistivat pilvipalveluiden syntymisen. [16]

Tärkeimpinä pilvipalveluita edeltävinä vaiheina Krutz & Vines (2010) erottelevat taulukon 2 mukaiset tekniikat.

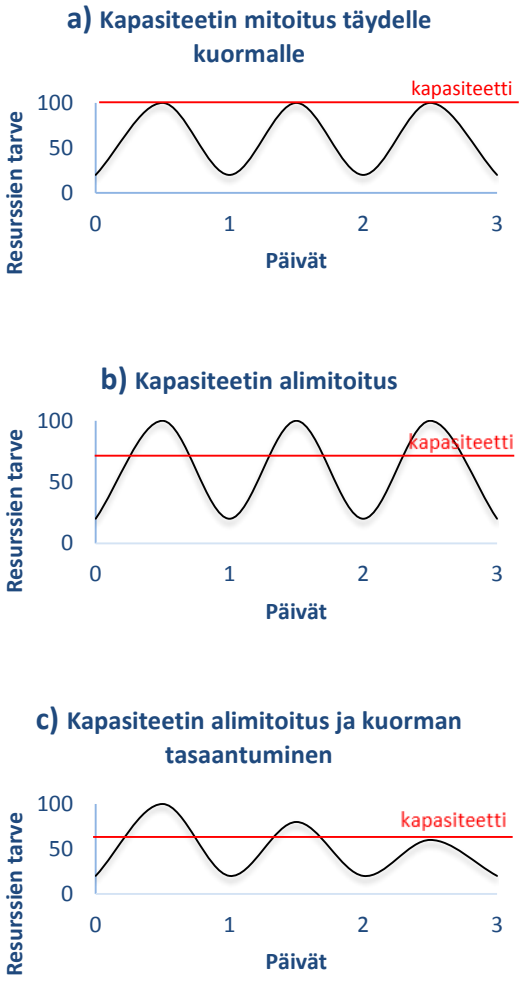
Taulukko 2: Tärkeimmät elementit, jotka edelsivät pilvipalveluita. [16]

Tekniikka	Kuvaus
Utility Computing = Tilausperustainen tietojenkäsittely	Tietojenkäsittelyresurssien paketointi ja jakelu asiakkaalle, joka maksaa käyttämistään resursseista. Tavoitteena on saada palvelut tehokkaammin käyttöön ja samalla vähentää kustannuksia. Sana "utility" kuvastaa tavoitetta, jossa tietokoneresurssit ovat samanlaisia hyödykkeitä kuin esimerkiksi sähkö ja kaasu.
Grid Computing = Verkkolaskenta	Käyttää useiden verkottuneiden tietokoneiden prosessointitehoa ratkaistakseen laskutoimituksia. Verkkolaskennassa palvelimet, levytila ja verkot muodostavat yhdessä tehokkaan laskentasolmun, joka voidaan ottaa dynaamisesti käyttöön tarpeen mukaan.
Autonomic Computing = Itsenäinen tietojenkäsittely	Tietojärjestelmän täytyy toimia ilman ulkoista kontrollointia. Termi viittaa ihmiskehon autonomiseen hermostoon, joka säätelee muun muassa hengitystä ja sydämen toimintaa ilman ihmisen tietoista toimintaa.
Platform Virtualization = Alustan virtualisointi	Looginen fyysisen tietokoneen osiointi usean tehtävän ajon alustaksi, koskien niin palvelimia, ohjelmistoja kuin käyttöjärjestelmiäkin. Virtualisoinnissa useita virtuaalikoneita käytetään samalla fyysisellä palvelimella.
Software as a Service (SaaS) = Ohjelmistot palveluna	Ohjelmistojen jakelun ja levittämisen malli, jossa ohjelmat tarjotaan asiakkaalle palveluna. Ohjelmat voivat pyöriä käyttäjän tietokoneilla tai suoraan tarjoajan Web-palvelimilla. SaaS tarjoaa tehokkaan päivitystenhallinnan sekä tukee yhteistyötä.
Service Oriented Architectures (SOA) = Palvelukeskeinen arkkitehtuuri	Ryhmä palveluita, jotka kommunikoivat keskenään, liitynnät ovat tunnettuja ja kuvattuja, toiminnot ovat löyhästi paritettuja (liityntä ei ole sidottu yhteen toteutukseen) ja palveluita voidaan hyödyntää useissa organisaatioissa.

Pilvipalveluita sovelletaan useisiin erityyppisiin palveluihin. Yhteinen ja tärkein ominaisuus pilvipalveluille on taustalla olevien palvelinten virtualisointi. Virtualisointi muuttaa palvelimen toiminnan ”tietokone, joka suorittaa prosesseja ja tarjoaa palveluita muille tietokoneille” -mallista muotoon ”prosessi, joka tarjoaa palveluita muille prosesseille”. Tämä prosessi voidaan suorittaa useissa koneissa samanaikaisesti ja on hajautettavissa useiden sijaintien kesken. Virtualisointiin liittyy myös vahvasti nopea joustavuus, joten sillä saadaan joustavasti varmistettua riittävät resurssit myös ruuhkahuippuja varten. [13]

Pilvitoimintamallissa usean käyttäjän ympäristössä virtuaalisten palvelinten avaus- ja lopetusmaksut saadaan pyöristettyä nollaksi, mikä mahdollistaa pilvipalveluiden avaamisen ja laskutuksen käytön mukaan. Tämä virtuaalikoneiden nopea skaalautuvuus on ollut tärkeimpiä vaiheita pilvitoimintamallin kehittymisessä. [10]

Pilvitoimintamalli mahdollistaa kapasiteetin oikean mitoituksen myös vaihteleville käyttäjämäärille. Staattisella palvelinympäristöllä toteutetuissa palveluissa resursseja jää aina osin hyödyntämättä, ja jos palvelu halutaan mitoittaa täydelle käyttäjämäärälle, toteutuksesta tulee hyvin raskas. Usein palvelun käyttäjämäärien tarkka ennustaminen on lähes mahdotonta, ja alimitoitetussa palvelussa osa käyttäjistä jää palvelun ulkopuolelle. Ajan mittaan osa ulkopuolelle jääneistä käyttäjistä ei enää palaa palvelun pariin, ja täten kuorma tasoittuu itsestään alemmalla tasolle, mikä tietää samalla yritykselle menetettyjä asiakkaita (kuva 7). [11]



Kuva 7. Riittävän kapasiteetin määrittäminen staattisella menettelyllä aiheuttaa aina resurssien hukkaamista (a). Jos mitoitusta ei tehdä huippujen mukaan (b), ajan myötä palvelun kuorma tasaantuu menetettyjen käyttäjien kautta (c). [11]

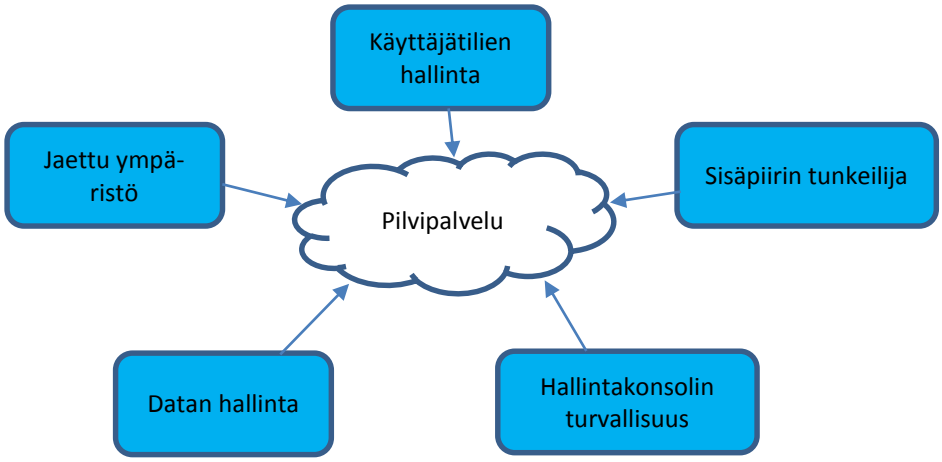
2.4 PALVELUIDEN TURVALLISUUS

Monet yritykset ajattelevat edelleen, että heidän oman palomuurinsa takana olevat sisäverkon ratkaisut ovat ainoa oikea tapa toimia. Kuitenkaan se, että palvelut sijaitsevat omassa sisäverkossa, ei välttämättä tuo juurikaan lisäturvaa. Lähes kaikki laitteet ovat nykyisin kiinni internetissä, ja samalla aukeavat monet tietoturvauhkat, joita vastaan tulisi suojautua. Yksittäinen väärin suojattu päätelaite voikin olla se, joka pilaa muuten hyvin toteutetun verkon tietoturvan.

Perinteiset tietoturvan elementit pätevät yleisesti myös pilvipalveluiden suhteen. Nämä elementit ovat tietojen luottamuksellisuus ja tietoturva, tietojen eheys, todentaminen ja saatavuus. Vaikka turvallisuusuhat eroavat perinteisen IT-ympäristön uhkakuvista, lähtökohdiltaan pilvipalveluita voidaan pitää tietoturvallisempina ratkaisuina kuin perinteistä pk-yrityksen ylläpitämää palvelinympäristöä. Pilvipalveluiden toteutustapa hyödyntää uusimpia turvallisuusohjeita ja tuo mukanaan keskitetyt datakeskukset ja yhdenmukaisen arkkitehtuurin. Homogeenisia palveluita tarjotaan pitkälti automatisoidun virtuaalialustan päältä, jolloin palveluntarjoaja voi keskittää resursseja itse arkkitehtuurin suojaamiseen huomattavasti mittavammilla resursseilla kuin mikään yksittäinen taho. [17]

Turvallisuushuolia voi aiheuttaa myös datan fyysinen sijainti. Mahdollinen sijainti voi määräytyä jo datan tai yritykset luonteesta johtuen, jolloin esimerkiksi tiedon tulee pysyä Suomen rajojen sisäpuolella tai EU-alueella. Usein tämä on yrityskäytössä ratkaistu siten, että käyttäjä voi valita, mihin maanosaan yrityksen tiedot tallennetaan.

Vaikka pilvitoimintamalli tuo luonnostaan useita turvallisuushyötyjä kuten keskitetyn turvallisuuden hallinnan, datan ja prosessien segmentoinnin, tiedon katoamisen turvaamisen ja korkean saavutettavuuden, on sillä infrastruktuurin liittyviä muita turvallisuusuhkia. Pilvitoimintamalliin kohdistuvat uhkakuvat Zissis & Lekkas (2012) jakavat kuvan 8 mukaisesti viiteen kategoriaan. [17]



Kuva 8. Pilvipalvelun uhkakuvien jaottelu viiteen eri pääkategoriaan. [17]

Turvallisuus yleisellä tasolla koostuu luottamuksellisuudesta, tietojen eheydestä ja saavutettavuudesta. Näiden kolmen laaja-alaisen vaatimuksen tulee toteutua niin datan, ohjelmistojen kuin myös rautatason suojauksessa. [17]

Vain hyväksytyillä osapuolilla tulee olla pääsy järjestelmään ja sen dataan. Pilvipalveluissa käyttäjiä on kuitenkin yleensä useita, joten myös datan väärinkäytön mahdollisuudet kasvavat. Järjestelmän käyttöoikeudet määritellään käyttäjän tunnistuksen perusteella, joten käyttäjätilien suojaaminen on erityisen tärkeää. Tilien suojaaminen korostuu entisestään pilvipalveluissa, joissa kaikkialta Internetistä on pääsy tietoihin. Pilvipalveluissa tulisikin käyttää vahvaa käyttäjätilien suojausta. [17]

Datan suojaamisen ohella yhtä tärkeässä asemassa ovat ohjelmistojen luotettavuus. Käyttäjän tulee luottaa siihen, että käytettävä sovellus käsittelee tietoja luotettavasti [17]. Tämä on muodostunut ongelmaksi erityisesti mobiilipuolella, jonka sovelluksista useat toimivat nykyisin pilvitoimintamallin mukaisesti. Sovellukset pyytävät asennettaessa käyttöoikeuksia laitteen eri resursseihin, ja käyttäjällä ei ole varmuutta siitä, mihin näitä tietoja käytetään. Jos oikeuksia ei anna, ainut keino on olla käyttämättä kyseistä sovellusta. [18]

Pilvitoimintamalli perustuu toimintatavalle, jossa käytetään jaettuja resursseja. Vaikka osapuolet on erotettu toisistaan virtualisointitasolla, taustalla olevat fyysiset palvelimet ovat yhteisiä. Tämä saattaa aiheuttaa tietoturvaongelmia huonosti toteutetuilla uudelleenkäytettävillä osioilla. Erityisesti ongelmia saattaa tulla jo poistetun datan tallennustilan uudelleenjakamisessa. Huonosti toteutettu datan tuhoaminen tai levytilan suojaaminen saattaa aiheuttaa yrityksen datan ajautumisen väärien henkilöiden käsiin. [17]

Tiedon luottamuksellisuuden ja tietoturvan rooli korostuu pilvipalveluissa. Tiedot on pilvipalveluissa tallennettu useisiin sijainteihin ympäri maapallon. Jo pelkästään tämä luo useita lainopillisia ristiriitoja datan tietosuojan suhteen. Lisäksi tiedon hajauttaminen luo lisää riskejä tiedon luottamuksellisuuden säilyttämiselle. Esimerkiksi eurooppalainen laki määrää, että organisaation tulisi tietää, missä henkilökohtainen data kulloinkin sijaitsee. [17]

Tietojen eheydellä tarkoitetaan sitä, että vain todennetuilla osapuolilla on pääsy tietoihin ennalta määritettyjen oikeuksien mukaisesti. Tämä koskee niin dataa, ohjelmistoja kuin myös laitteistoympäristöä. Valvomalla yrityksen järjestelmiin pääsyä ja oikeuksia voidaan estää tietojen väärinkäytökset ja varkaudet. Lisäksi oikeuksien valvonnalla saadaan tietoon, kuka tietoja on milloinkin käsitellyt. Pilvitoimintamallissa palvelun tarjoajan tehtävänä on huolehtia tietojen eheydestä ja virheettömyydestä. [17]

Järjestelmien ja tiedon saavutettavuus tunnistetuille käyttäjille haluttuna aikana on pilvipalveluiden yksi tärkeimmistä vaatimuksista. Pilvipalveluiden saavutettavuus tulee olla varmistettu myös tilanteissa, joissa samaa pilvipalvelua käyttävät mahdolliset rikollistahot yrittävät tunkeutua järjestelmään tai muuten aiheuttavat toiminnallaan tietoturvariskejä järjestelmää kohtaan. Saavutettavuuden vaatimus koskee niin dataa, ohjelmistoja kuin myös laitteistoja. Saavutettavuudessa aina käytettävissä olevan internetyhteyden rooli korostuu. Vain tietoverkon kautta pilvipalvelun käyttäjän on mahdollista päästä käsiksi palvelussa oleviin tietoihin tai suoritettaviin ohjelmiin. [17]

2.5 LUOTTAMUKSEN RAKENTUMINEN PILVITOIMINTAMALLISSA

Luottamusta on tutkittu jo pitkään tietojenkäsittelytieteistä puhuttaessa. Pilvitoimintamallissa luottamuksen syntymiseen vaikuttaa vahvasti se, millä tasolla pilvipalvelu toimii, eli häviääkö datan ja ohjelmistojen hallittavuus pilvipalvelun toteuttavan yrityksen haltuun (SaaS) vai säilyykö se osin yrityksellä (PaaS ja IaaS). Pilvipalveluiden osalta luottamuksen syntyminen poikkeaa perinteisen IT-infrastruktuurin toteutustavasta oleellisesti. Perinteisissä talon sisäisissä järjestelmissä luottamuksen syntymiseen voidaan vaikuttaa tiukasti toteutetuilla turvallisuussäännöstöillä, jonka mukaan tiedostojen ja ohjelmistojen käyttö määräytyy. Pilvitoimintamallissa kontrolli säännöstöjen oikeaoppisesta toteutuksesta siirtyy palvelun toteuttavan yrityksen tehtäväksi. [17]

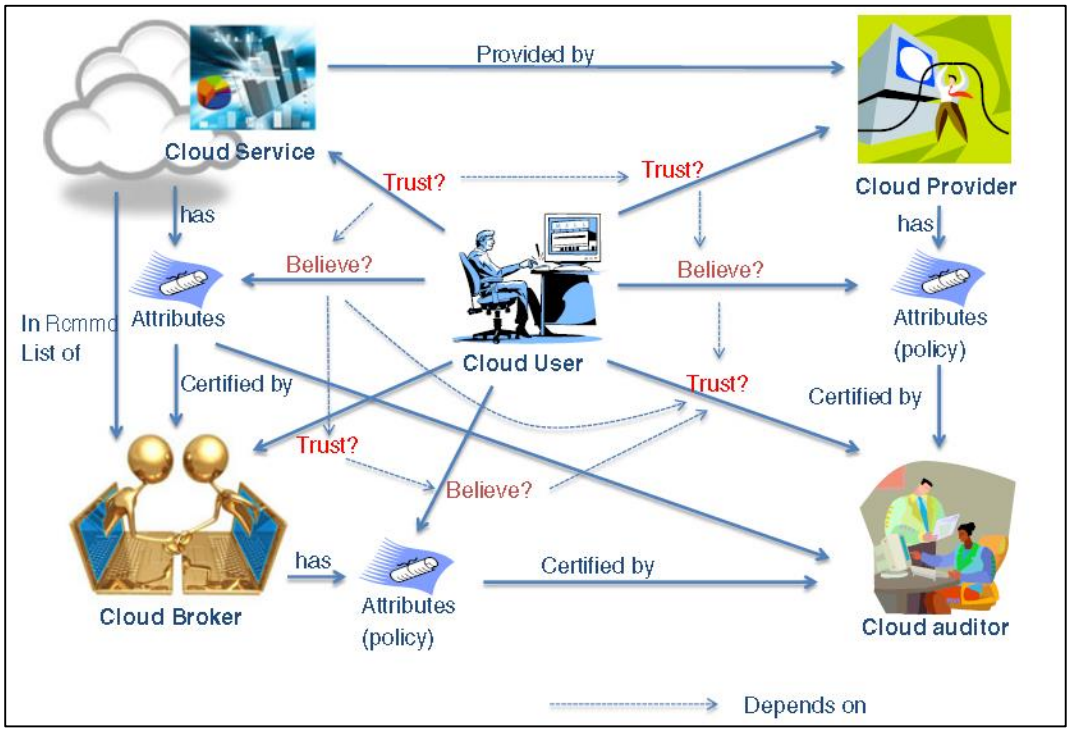
Luottamuksen syntymiseen vaikuttavia tekijöitä on useita. Huang & Nicol (2013) erottelevat tutkimuksessaan viisi pääkohtaa, jotka voivat edesauttaa luottamuksen syntymistä (taulukko 3). [19]

Taulukko 3. Luottamuksen syntymistä edesauttavia toimia pilvipalveluille. [19]

Luottamuksen perusta	Kuvaus
Yrityksen maine	Yhteisöjen sisällä syntynyt maine ohjaa yhteisön luottamusta yritykseen
SLA (Service Level Agreement) -palvelutasot ja QoS (Quality of Service) -laatutason määritykset	Sopimuksella määritetyt palvelutasot tuotteen saatavuudelle ja laadulle
Palveluiden läpinäkyvyys	Yrityksen toimien avaaminen kuluttajille. Useita eri palveluita otettu käyttöön.
Luottamus kolmannen osapuolen järjestelmän kautta (Trust as a Service, TaaS)	Käyttäjän luottama palveluntarjoaja käyttää omassa palvelussaan toisen palveluntarjoajan järjestelmiä hyväkseen
Akkreditoinnit, auditoinnit ja standardit	Luotetun osapuolen tekemät viralliset arvioinnit

Pilvipalvelun käyttäjä joutuu useiden valintojen eteen päättäessään tarjotun palvelun luotettavuudesta. Huang & Nicol kuvaavat tätä toimintaa luottamuksen ketjuksi

(kuva 9). Ensin käyttäjän tulee päättää luottamuksesta palvelun tekniseen ratkaisuun (kuvassa 9, cloud service), jolla on ilmoitetut ja mahdollisesti sertifioidut ominaisuudet, joiden toimivuuteen käyttäjän tulee luottaa. Samoin käyttäjän tulee luottaa palvelun toteuttavaan osapuoleen (kuvassa 9, cloud provider) sekä mahdolliseen välittäjäosapuoleen (kuvassa 9, cloud broker) ja näiden julkaisemiin palvelutietoihin. Koska toteutusten ominaisuuksiin luottaminen tapahtuu sertifiointien ja auditointien kautta, edellyttää se myös luottamusta auditoinnin suorittaneeseen osapuoleen (kuvassa 9, cloud auditor). [19]



Kuva 9: Luottamuksen syntyminen pilvipalveluissa vaatii luottamuksen syntymistä koko palveluketjua kohtaan. [19]

Pilvitoimintamallin tarjoajille on myös tärkeää toteuttaa ratkaisunsa luotettavasti ja hyväksi havaittuja käytäntöjä noudattaen. Pilvipalvelu voi toimia vain, jos sillä on riittävästi käyttäjiä, ja asiakkaat pysyvät palvelun käyttäjinä vain, jos he kokevat sen turvalliseksi käyttää. Jos palveluista käy ilmi, että palvelut eivät täytä vaadittuja tietoturvatasoja tai ne hukkaavat käyttäjiensä tietoja, asiakkaat poistuvat palvelun piiristä. Näin tapahtuu myös, jos palvelun saavutettavuus on heikko. [20]

Luottamus pilvipalveluihin koki kovan kolauksen 7.6.2013, kun The Guardian -lehti julkaisi ensitietoja Edward Snowdenin vuotamista NSA:n (National Security Agency) vakoilutiedoista. Vakoiluohjelma paljastui, kun NSA:n entinen työntekijä Edward Snowden luovutti The Guardian ja The Washington Post -lehdille salaiseksi luokiteltua tietoa, jota oli kerätty maailmanlaajuisesti PRISM-ohjelman avulla. Julkaistun tiedon mukaan NSA:lla on suora pääsy Googlen, Facebookin, Applen ja useiden muiden suurten yritysten käyttäjätietoihin. Myös Microsoftin palveluiden tietoihin on vuotaneiden asiakirjojen mukaan ollut jonkinasteinen pääsy. [21]

Paljastuksen jälkeen yritykset ovatkin tehneet kaikkensa, jotta luottamus palveluihin palautuisi. Monet yritykset ovat tiedotteissaan kiistäneet automaattisen pääsyn järjestelmiinsä, ja kaikki tiedot järjestelmästä on saatu vain erillisillä lain mahdollistamilla pyynnöillä. Yritykset haluavatkin Yhdysvaltain valtion kertovan julkisesti avoimemmin, minkälaisia määriä, mitä sekä miten tietoja on kerätty. Tämä on erityisen tärkeää vahvasti luottamukseen perustuvan toimialan toiminnan kannalta. [22]

Yhdysvaltojen pilvitoimintamallin yrityksille NSA:n tietovuoto tietää tulevina vuosina suuria rahanmenetyksiä. Paljastus vaikutti välittömästi pilvipalveluihin siten, että niitä siirtyi pois Yhdysvalloista ja vaikutuksen uskotaan kestävän pitkään. Euroopan valtioilla onkin nyt hyvä mahdollisuus kiriä kiinni Yhdysvaltojen etumatkaa pilvipalveluissa. [23]

Vakoilutapauksen paljastuminen on jo muuttanut monia pilvipalveluita ja näin tapahtuu jatkossakin. Microsoftin suhteen uutisoinneista ei tarkalleen selviä, millä tasolla NSA on tietoihin päässyt ja rajoittuiko pääsy pelkästään kuluttajapuolen palveluihin. Esiin ovat kuitenkin nousseet Googlen ja Yahoon tietojen keräyksen yhteydessä myös Microsoftin online-palvelut ja Hotmail-sähköpostin osoitekirjan tietojen keräys. Yrityksistä Google ja Yahoo ovatkin päättäneet laajentaa kryptauksen käyttöä palveluissaan. [24]

Myös Microsoft ilmoitti 4.12.2013 blogissaan tehostavansa kuluttajadatan suojausta valtioiden vakoilua vastaan. Microsoft ilmoitti parantavansa palveluitaan kolmella eri alueella:

- Laajentavat salauksen käyttöä kaikissa palveluissaan
- Käyttävät kaikkia lain sallimia mahdollisuuksia kuluttajien datan suojaamiseksi
- Parantavat ohjelmistojen koodin läpinäkyvyyttä, jotta käyttäjät voivat varmistua ohjelmistojen olevan vapaita takaovista

[25]

2.6 PILVIPALVELUIDEN KÄYTTÖÖNOTON VAIKUTUKSIA YRITYKSEN TIEDONHALLINTAAN

Pilvipalveluiden käyttöönotto vaikuttaa erityisen houkuttelevalta pk-yrityksien näkökulmasta. Suuryritysten kohdalta tilanne voi olla toinen. Yrityksen oman palvelinsalin tuottamat palvelut ovat yleensä isolle joukolle edullisempia kuin kuukausihintainen palvelumaksu pilvipalveluista. Suuryrityksillä on yleensä myös omaa vanhempaa laitekantaa, jota pitäisi pystyä hyödyntämään myös uusien järjestelmien rinnalla. Tällöin kyseeseen voi tulla hybridimalli, jossa osa palveluista otetaan pilvipalvelun kautta ja kriittinen data pidetään yrityksen omassa palvelinsalissa. Monilla yrityksillä tämän määrityksen voi sanella myös hyvin korkeaksi asetettu SLA-palvelutaso, johon kaikki pilvipalvelut eivät vielä yllä. Samanaikaisesti pilvipalvelujen SLA-taso on kuitenkin paljon korkeampi, kuin mihin pk-yritys kykenee omassa infrastruktuurissaan. [9]

Yritykset perustelevat usein tietoturvan näkökulmasta siirtymättömyyttään pilvipalveluihin. Tämä on ymmärrettävä peruste, sillä siirtymisen myötä yrityksen data siirtyy yrityksen omista tiloista kenties sijainniltaan tuntemattomaan palvelinsaliin. Tämän vuoksi yritykset eivät ole olleet innokkaita siirtämään tietojaan oman yrityksensä ulkopuolelle.

Pilvipalveluihin siirtymisessä on kuitenkin sovelluskohtaisia eroja. Toisien sovelluksien pilvipalveluihin siirtämisen hyödyt ovat selvästi nähtävissä, joten palvelut

tuntuvat houkuttavimmalta perinteisiin palvelinratkaisuihin nähden. Esimerkiksi sähköpostit sisältävät usein erittäin tärkeää tietoa, jonka päätyminen ulkopuolisten käsiin tulisi estää. Kuitenkin sähköpostisovelluksia pidetään usein ensimmäisinä harppauksina kohti muita pilvipalveluita, ja tällä on mahdollisesti suuria vaikutuksia yrityksen halukkuuteen siirtyä kohti muita yritystä hyödyntäviä pilvipalveluita. [26]

Sähköpostipalvelujen siirtäminen pilvipalveluun muuttaa yrityksen käytäntöjä sähköpostin käsittelyssä. Se tuo mukanaan niin hyviä kuin myös joitakin lisäpohdintaa aiheuttavia asioita.

Hyödyt:

- Pilveen keskitetyt sähköpostipalvelut tuovat yrityksen käyttöön keskitetyt hallinta- ja raportointityökalut. Keskitetyt tietoturvasäännöt mahdollistavat nopeasti hyväksyttyjen käytäntöjen käyttöönoton koko organisaatiossa. Samalla valmiit raportointityökalut vähentävät yrityksen IT-osaston taakkaa.
- Tehokkaat roskaposti- ja haittaohjelmasuodatukset säästävät yrityksen tietoliikennekaistaa, kun suodatus tapahtuu jo pilvipalvelussa eikä vasta yrityksen sisäverkossa.
- Järjestelmä on aina ajan tasalla.

Tietoturvahuolet ja muut yrityksissä pohdintaa aiheuttavat kohdat:

- Yritys menettää monessa tapauksessa kontrollin työkaluihin, joilla voitaisiin valvoa datan käyttöä. Näitä ovat muun muassa käyttäjätilastot, systeemin lokitiedot sekä muut lokien kautta nähtävät tietoturvauhkat.
- Jos käytetään peruspalvelusta erillisiä, tietoturvallisempia datakeskuksia, voi aiheutua ylimääräistä viivettä tiedonsiirrossa.
- Jaettuja resursseja käytettäessä mahdolliset DoS (Denial of Service) -hyökkäykset voivat aiheuttaa ongelmia muilla kuin alkuperäisessä kohteessaan.
- Pilvipalvelut paljastavat ICT-järjestelmien piilotetut kulut, joita ei aina osata laskea mukaan käytettäessä talon sisäisiä järjestelmiä.

[26]

Wieland ei käsitellyt artikkelissaan yhtä hyvinkin ilmeistä syytä sähköpostin siirtämiselle pilvipalveluun. Pilvipalvelun kautta sähköposti on saavutettavissa helposti kaikkialta ja kaikilla laitteilla ajantasaisen järjestelmän kautta. Tämä helpon mobiilin sähköpostin tarve lienee ollut yksi suurimmista yksittäisistä tekijöistä pilvisähköpostipalvelujen yleistymiseen.

Sähköpostin välityksellä jaetaan edelleen paljon tiedostoja, mikä johtaa tietojen hajautumiseen ja siihen, että jokaisella käyttäjällä on omat versiot samoista organisaation tiedostoista. Sähköpostin käyttäminen tiedostojen siirtokanavana kasvattaa nopeasti yrityksen tiedonsiirtokaistan ja tallennustilan tarvetta. Yrityksissä syntyy kiihtyvää tahtia uusia dokumentteja, ja sähköpostin sekä perinteisten jaettujen levytilojen käyttö tiedon jakamiseen vaikeutuu. Tämä jatkuva tiedon määrän kasvaminen ajaa yritykset kohti yrityskohtaisia sisällönhallintajärjestelmiä (ECM, Enterprise Content Management). Tiedon pitää myös olla aina saavutettavissa, joten pilvitoimintamallin mukaiset ratkaisut yhteistyön ja dokumenttienhallinnan parantamiseen ovat yrityksiä kiinnostava yhtälö. [27]

Sisällönhallintajärjestelmällä yritykset pyrkivät saamaan yrityksessä levällään olevan tiedon keskitettyä yhteen paremmin hallittuun järjestelmään, jonka kautta tieto saataisiin jaettua sitä tarvitseville nopeammin ja tarkemmin. Sisällönhallintajärjestelmän avulla tarvittava tieto on löydettävistä aina yhdestä paikasta ajantasaisena versiona.

Perinteisesti kaikki yrityksen palomuurien sisäpuolella olevat tiedot ovat ulkopuolisilta suojatut ja pääsy näihin vaatii pääsyn yrityksen verkkoon. Tiedostojen jakaminen ja käyttäminen useilla päätelaitteilla on usein monimutkaista ja vaikeaa, mikä on aiheuttanut yrityksissä niin kutsutun Dropbox-ongelman – käyttäjät ottavat yritysdatan jakamiseksi käyttöön samoja ohjelmistoja, joita he ovat tottuneet käyttämään henkilökohtaisessa käytössään. Käyttäjän henkilökohtaisien sovellusten kautta jaettu data ei ole millään tavalla yrityksen hallinnassa, ja viimeinenkin kontakti dataan häviää työntekijän poistuessa yrityksestä. Pilvipohjaisilla sisällönhal-

lintajärjestelmillä voidaan tarjota sama tiedostojen ja tietojen jakaminen myös yrityksen ulkopuolelle, mutta erona on se, että yritys päättää, mitä tietoja voidaan jakaa ja kenelle. [28]

Sisällönhallintajärjestelmien palvelinvaatimukset ovat usein massiiviset ja näin ollen pk-yritysten ulottumattomissa. Pilvipalveluiden kuukausipohjainen veloitus tuokin ennen vain suuryritysten saavutettavissa olleet yhteistyö- ja tiedonjakamisen alustat kaikkien halukkaiden käyttöön. Lisäksi pilvipohjaiset ratkaisut voivat lisätä järjestelmän suorituskykyä resurssien nopean skaalautuvuuden kautta. Dhouib ja Halima (2013) tekivät vertailevan testin Microsoftin SharePoint-alustan suorituskykyeroista perinteisen oman palvelimen ja pilvitoimintamallin välillä. Mitä useampia tehtäviä alustalla suoritettiin, sitä parempi oli pilvipalveluiden suorituskyky verrattuna omaan palvelimeen. Pilvipalveluiden avulla palvelinten kuormaa saadaan skaalattua nopeasti tarpeenmukaiselle tasolle. [27]

Jos yritys päättää siirtyä pilvipohjaisiin sähköposti- ja sisällönhallintajärjestelmiin, tarkoittaa se samalla myös sitä, että päätelaitehallintaa pitää pohtia uudelleen. Koska pilvipalveluissa yrityksen tietoihin on pääsy lähes kaikilta Internet-yhteyden omaavilta päätelaitteilta, tulee päätelaitehallinnan kyetä hallitsemaan näitä laitteita riippumatta niiden sijainnista. Yrityksen oman verkon sisällä toimivien hallintaratkaisujen rajat tulevat usein vastaan poistuttaessa oman Active Directoryn -alueelta tai viimeistään useiden eri mobiililaitteiden kohdalla. Tällaisessa tapauksissa hallintarajoja voidaan kasvattaa VPN- tai Direct Access -yhteyksien avulla sekä erillisen MDM (Mobile Device Management) -ohjelmiston avulla.

Toinen ja paremmin muita pilvipalveluita tukeva keino on ottaa myös päätelaitehallinta pilvitoimintamallin mukaisesti palveluna. Tällöin on mahdollista saada kaikki päätelaitteet saman hallinnan piiriin, mikä helpottaa raportointia hälytyksistä ja vikatilanteista sekä asennetuista ohjelmistoista.

3 MICROSOFTIN PILVIPALVELUT YRITYKSILLE

Microsoft on ollut lähes yksinvaltiaan asemassa PC-puolen käyttöjärjestelmien ja toimistosovellusten toimittamisessa jo 1990-luvulta asti. Työasemakäytössä Windowsin eri versioita on edelleen käytössä liki 91 %:ssa koneita. Windowsin asemaa on viime vuosina horjuttanut lähinnä Applen voimakas suosio niin kannettavien tietokoneiden kuin myös tabletti- ja matkapuhelinrintamalla. Tietokoneissa Applen iOS-käyttöjärjestelmää käyttää noin 7,5 %. Ilmaisen Linux-käyttöjärjestelmän suosio on pysähtynyt noin 1,5 % tietämille. [29]

Toimistosovelluksissa Microsoft on ollut vähintään yhtä suositussa asemassa. Vuonna 2006 Microsoft sai varteenotettavan kilpailijan toimistosovellusten suhteen, kun Google julkaisi pilvipalveluna tekstinkäsittely- ja taulukkolaskentaohjelmistot [30]. Google Docs on henkilökohtaisessa käytössä ilmainen ohjelmisto ja yrityksillekin huomattavasti edullisempi verrattuna Microsoftin toimistosovelluksiin. Microsoft vastasi Googlen aloittamaan online-sovellusten tuloon vasta vuoden 2010 Office-julkistuksen myötä, joka toi vihdoin myös mahdollisuuden muokata tiedostoja suoraan verkosta käsin. [31]

Microsoftia ja Googlea verrattaessa kilpailutilanne on hieman erilainen. Microsoftin tulot pohjautuvat pitkälle käyttöjärjestelmiin ja toimistosovelluksiin, kun taas Google saa suurimman osan tuloistaan mainostuloina. Microsoft onkin joutunut mukaan hintakilpailuun, jotta saisi pidettyä asiakkaat Office-tuoteperheen parissa. Esimerkiksi 2013 vuoden joulukuussa Microsoft tarjosi koulujen oppilaille ilmaiset Office 365 -ohjelmistot käyttöön vastaiskuna Googlen Chromebook-tietokoneiden ja Google Appsin-yhdistelmälle. [32]

Muuttuvassa markkinatilanteessa osuuksien pitäminen samalla korkealla tasolla niin käyttöjärjestelmien kuin toimistosovellusten osalta on haastavaa. Vielä muutama vuosi sitten pilvipalveluilla tarjottavien ohjelmistojen ominaisuudet olivat paljon jäljessä perinteisiä ohjelmistopaketteja. Tällä hetkellä tilanne on kääntymässä päinvastaiseksi, ja monissa sovelluksissa uusimmat ominaisuudet tulevat jo ensin

pilvitoimintamallin ohjelmistoihin ja vasta tämän jälkeen vastaaviin työpöytäsovelluksiin. Microsoftille onnistunut siirtyminen perinteisistä ohjelmistoista pilvipalveluihin onkin erittäin tärkeää. Tästä osaltaan kertoo jo se, että Microsoftin uudeksi toimitusjohtajaksi valittiin entinen pilvipalveluosaston johtaja, Satya Nadella [33].

Satya Nadella piti pian toimitusjohtajaksi valitsemisensa jälkeen 27.3.2014 puheen, jossa hän julkaisi Microsoftin uuden strategian, joka on tiivistettävissä lauseeseen: ”Mobile first, Cloud first”. Nadella täsmentää lauseen tarkoittavan mobiililaitteita, eikä vain matkapuhelimia vaan mitä tahansa laitteita, jotka kaikki tulevat kytkeytymään pilvipalveluun saumattomasti. Käyttäjä tulee saamaan saman käyttökokemuksen laitteesta riippumatta. [34]

3.1 MICROSOFT AZURE

Microsoftin pilvipalveluiden voidaan katsoa alkaneen Azure-alustan julkistamisesta vuonna 2008 [35]. Windows Azure, jonka nimi muuttui huhtikuussa 2014 Microsoft Azureksi, tarjoaa käyttäjille PaaS- ja IaaS-tarjoaman mukaisen pilvipalvelualustan. Sen päälle voidaan rakentaa sovelluksia lähes kaikilla ohjelmointikielillä ja eri alustoille sekä selaimille. Azuren palvelut on jaoteltu taulukon 4 mukaisesti. [36]

Taulukko 4. Microsoft Azuren palveluiden jaottelu eri osa-alueiden mukaan. [36]

Laskenta (Compute)	Datapalvelut (Data services)	Sovelluspalvelut (App services)	Verkot (Networks)
- Virtuaalikoneet - Pilvipalvelut - Web-sivustot - Mobiilipalvelut	- Tallennustila - SQL-tietokanta - HDInsight-analysointi - Välimuisti - Palautuminen	- Mediapalvelut - Palveluiden yhdistäminen - Tiedotusten julkaisu - Ajoitetut tehtävät - BizTalk-prosessit - Active Directory - Monivaiheinen tunnistus	- ExpressRoute - yhteydet verkkojen välillä - Virtuaaliverkot - Verkkoliikenteen hallinta

Microsoft Azure on yrityksille helppo ja edullinen ratkaisu jatkaa oman konesalinsa kapasiteettia pilvipalveluihin. Palveluista maksetaan pilvipalveluperiaatteen mukaisesti vain käyttöajalta, joten suurenkin hetkittäisen kapasiteetin tarve on toteutettavissa kohtuullisin kustannuksin. Microsoftin mukaan jo 54 % Fortune 500 -listan yrityksistä käyttää Azurea osana liiketoimintaansa [36].

Microsoft Azuren päällä toimii myös Office 365:den ja Windows Intunen käyttäjätietokanta, Windows Azure Active Directory (WAAD). Yrityksessä jo mahdollisesti oleva Active Directory (AD) -tietokanta voidaan synkronoida DirSync-työkalun avulla Azuren AD:hen. Tämän synkronoinnin avulla voidaan ottaa käyttöön kertakirjautuminen Microsoftin palveluihin, kuten myös useisiin muiden valmistajien pilvisovelluksiin. [36]

Kuten olen aiemmin todennut, pilvipalveluiden välillä käydään kovaa kilpailua asiakkaista. Yritykset koittavatkin parhaansa mukaan erottua ja vakuuttaa käyttäjät palveluidensa paremmuudesta ja turvallisuudesta. Myös Microsoft Azuren pilvitoimintamallin arviointiin on olemassa useita kolmannen osapuolen auditointeja (taulukko 5).

Taulukko 5. Microsoft Azuren pilvitoimintamallin määräysten mukaisuuden todentaminen tapahtuu suurelta osin kolmansien osapuolien todistusten kautta. [37]

Määräystenmukaisuuden todentanut kolmas osapuoli	Kuvaus
ISO/IEC 27001:2005 Auditointi ja sertifiointi	Laaja-alaisesti käytössä oleva kansainvälinen tiedonhallinnan standardi
SOC 1 ja SOC 2 SSAE 16/ISAE 3402 todistukset	Suunnittelun ja toteutuksen tehokkuutta sekä hallintaympäristöä ja sen tietoturvaa, saatavuutta ja luottamuksellisuutta
Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)	Yhdistetty arviointi, joka suoritetaan SOC 2 -auditoinnin yhteydessä. Luo läpinäkyvyyttä siihen, kuinka turvallisuuden hallinta on toteutettu ja hallittu.
Federal Risk and Authorization Management Program (FedRAMP)	Microsoftin julkinen pilvi on hyväksytty yhdeksi pilvipalveluiden alustaksi Yhdysvaltojen liittovaltion käyttöön
Payment Card Industry (PCI) Data Security Standards (DSS) Level 1	PCI-sertifiointi takaa turvallisen luottokorttiliikenteen käsittelyn
United Kingdom G-Cloud Impact Level 2 Accreditation	Iso-Britannian oma akkreditointi pilvipalveluille
HIPAA Business Associate Agreement (BAA)	Yhdysvaltojen lakien täyttäminen terveydenhoitoalan tietojen käsittelyssä

Myös pilvialustan tarjoajien välillä on käynnissä kova kilpailu. Alan selvä johtaja on jo vuosia ollut Amazon Web Services. Viime vuosina se on alkanut saada varteenotettavia kilpailijoita niin Googlesta kuin erityisesti Microsoftista. Kilpailu on vaikuttanut hintojen tippumiseen ja tarjottujen palvelujen paranemiseen. Kuvassa 10 on kuvattuna IaaS-palveluntarjoajien tuorein kilpailutilanne Gartnerin raportin mukaisesti. [38]

Kuva 10. IaaS- pilvipalvelumallin tarjoajat esitettynä nelikenttämallin avulla. Nelikenttämallissa oikeassa laidassa ovat kaikkein visionäärisimmät yritykset kun taas ylälaidan sijainti merkitsee kykyä toteuttaa palveluita. [38]

Gartnerin raportista on huomattavissa Amazonin selvä johtoasema pilvi-infrastruktuurin tarjoajana sekä Microsoftin yhtä selvä toinen sija. Microsoft panostukset Azure-ympäristöön ovat niin mittavia, että eron voidaan olettaa hyvällä syyllä kaventuvan tulevina vuosina.

3.2 OFFICE 365

Microsoftin ensimmäinen kaupallinen pilvipalveluna toimiva toimistosovellusratkaisu oli Microsoft Online Services, joka tunnetaan myös nimellä BPOS (Business Productivity Online Services). BPOS perustui Office 2007 -tuotteiden ympärille, ja se sisälsi Exchange-sähköpostin, nykyistä kevyemmän SharePoint-onlineversion, Office Communicatorin sekä Live Meeting -neuvottelupalvelun [39]. Vaikka BPOS sisälsi paljon samoja ominaisuuksia kuin tuleva Office 365, oli varsinkin sen hallittavuudessa ja käytettävyydessä paljon puutteita nykyisiin versioihin nähden.

Microsoftin vuonna 2011 julkaisema Office 365 toimii SaaS-pilvipalvelumallin mukaisesti. Se on saatavilla useina eri versioina käyttäjäkohtaiseen kuukausimaksuhintaan. Office 365 sisältää aina Exchange-isännöidyn sähköpostin, suojauksen roskapostilta ja haittaohjelmilta, sekä tilauksesta riippuen Lync-pikaviesti- ja verkkoneuvottelupalvelun, OneDrive for Business -tallennustilan, Office työpöytä- ja Online-sovellukset, SharePointin sekä paljon muita yrityksen viestintään tarkoitettuja osioita (liite 2). Office 365:dellä on merkittävä vaikutus siihen, kuinka nykypäivän yrityksissä työskennellään. Se tuo kaikki tutut työpöytäsovellukset käyttöön myös verkkosovelluksina, jolloin vastaavaa työpöytäsovellusta ei välttämättä tarvitse olla koneelle asennettuna. Verkkosovellusten käyttö mahdollistaa myös yhtäaikaisen työskentelyn saman tiedoston parissa.

Office 365 on saanut yhden suuren päivityksen, kun Office 2010 -version päälle rakennetut sovellukset vaihtuivat 2013 versioon. Tulevaisuudessakin Office 365 tulee käyttämään aina uusimpia versioita toimistosovelluksista. Office 365:den käyttö on alun perin tarkoittanut pilvipalveluiden käyttöä yhdessä työpöytätoimistosovellusten kanssa, mutta uusimmissa versioissa on menty jatkuvasti kohti ratkaisua, jossa pilvipalveluita voidaan käyttää täysipainoisesti ilman työpöytäsovelluksia. Online-ohjelmistojen päivitystahti onkin työpöytäversioita huomattavasti nopeampi. 19.2.2014 julkaistun päivityksen myötä ennen nimellä Office Web Apps tunnetut verkkosovellukset ovat nykyisin Office Online -sovelluksia. Samalla näiden toiminnot paranivat huomattavasti ja toiminta yhdenmukaistui eri selaimien välillä.

Office 365 on alun perin yrityksille ja yhteisöille suunnattu ratkaisu. Se mahdollistaa sisäisen kommunikaation ja tiedostojen jakamisen ilman tarvetta muodostaa monimutkaisia oman konesalin ratkaisuja. Office 365 mahdollistaa pääsyn käyttäjän tiedostoihin ja yhteistyötyökaluihin miltä tahansa tietokoneelta ja mobiililaitteelta. [20]

Office-tuotteita tarjotaan kahden eri pääkategorian alla. Jos pelkkä sähköposti on riittävä tuote, niin tähän tarkoitukseen Microsoft tarjoaa Exchange Onlinesta kolme

eri vaihtoehtoa. Office 365:den puolella vaihtoehtoja on viisi erilaista. Nämä palvelupaketit on jaoteltu yrityksen koon mukaisesti pieniin yrityksiin (1–10 henkilöä), keskisuuriin yrityksiin (10–250 henkilöä) ja suuryrityksiin (rajoittamaton). Vielä jokin aika sitten pakettien välillä vaihtaminen oli vaikeampaa, mutta tämä on muuttunut viimeisten päivitysten myötä, ja myös pienyrityspaketeista voidaan siirtyä suuryrityspaketteihin. [40]

Pien- ja keskisuurten yritysten palvelupakettien hinnoittelu vaihtelee ominaisuuksien mukaan 4,10 euron ja 12,30 euron välillä. Suuryrityksillä vaihteluväli on 6,50 € - 19,00 €:n välillä. Vaikka palvelupaketit on nimetty yrityksen kokoluokan mukaisesti, pystyvät kaikki yritykset valitsemaan heille sopivan palvelupaketin, kunhan vain käyttäjämäärät pysyvät määritettyjen ylärajojen alapuolella. [40]

Jos asiakkaalla ei ole uusimpia Office-työpöytäohjelmistoja, parhaan hyödyn Office 365:destä saa palvelupaketeilla, joissa mukana tulee uusin versio Office-sovelluksista. Tämän vuoksi käyttäjän on mahdollista asentaa Office-sovellukset viidelle eri käytössään olevalle laitteelle. Lisäksi Office-sovellukset sisältävä tilaus mahdollistaa uusimpien työpöytäsovellusten käytön missä tahansa tietokoneessa, johon käyttäjä tunnuksillaan kirjautuu. Microsoftin Office on Demand -palvelussa sovellukset virtautetaan käytössä olevaan tietokoneeseen siten, että käytöstä ei jää jäljelle mitään asennusohjelmia tai pikakuvakkeita, joten käyttö ei vaadi tietokoneen käyttäjältä järjestelmänvalvojan tunnuksia. Office on Demand -käyttöön riittää, että tietokoneella on pääsy Internetiin. [41]

3.2.1 EXCHANGE ONLINE

Office 365:den tunnetuin osa on isännöity Exchange-sähköposti. Se suojaa tehokkaasti käyttäjän sähköpostit roskapostilta ja haittaohjelmilta jo palvelinpäässä, jolloin viestit eivät koskaan päädy käyttäjän koneelle asti.

Suurin hyöty pilvipalvelun käyttämisestä sähköpostin yhteydessä on yrityksen sähköpostiin pääsy useiden eri laitteiden välityksellä. Postia voi käyttää paikallisesti asennetulla Outlook-ohjelmistolla, verkon kautta Outlook Online -ohjelmistolla

sekä lähes kaikkien mobiilipäätelaitteiden kautta sijainnista riippumatta. Lisäksi vaikka Exchange-palvelin sijaitsee pilvessä, palvelin tarjoaa laajat työkalut järjestelmänvalvojan käytettäväksi. [20]

Järjestelmän hallinnointi tapahtuu Exchange Administration Center -.portaalin kautta, josta käsin voidaan muun muassa määritellä yrityksen käytäntöjä tietohävikin estämiseksi sekä määritellä ja valvoa yrityksen mobiilikäytäntöjä.

3.2.2 SHAREPOINT ONLINE

SharePoint on palvelinpohjainen tietokantasovellus, jota käytetään enimmäkseen tiedostojen hallintaan, mutta se sisältää myös useita ryhmien yhteistyötä helpottavia työkaluja. SharePoint Online mahdollistaakin reaaliaikaisen yhteistyön web-liittymän kautta. [20]

SharePoint-alusta taipuu moneksi, ja kuvaavin termi lienee sisällönhallintajärjestelmä, ECM (Enterprise Content Management). Sisällönhallintajärjestelmien alalla toimivia yrityksiä on useita. Gartnerin tekemässä nelikenttämallista voidaan helposti havaita alan päätoimijat (kuva 10).

Kuva 11. Sisällönhallintajärjestelmien toimittajien vertailu nelikenttämallin avulla. Nelikenttämallissa oikeassa laidassa ovat kaikkein visionäärisimmät yritykset kun taas ylälaidan sijainti merkitsee kykyä toteuttaa palveluita. [42]

Kuten Gartnerin Magic Quadrant -raportin nelikentästä voidaan havaita, Microsoft on yksi johtavista sisällönhallintajärjestelmien tuottajista. Microsoftin SharePoint onkin muotoutunut lähes standardiksi yritysten intranet- ja yhteistyöalustana. Vuonna 2011 Microsoft kertoi SharePointin olevan käytössä 78 %:lla Fortune 500 -listan yrityksistä. [43]

SharePoint Online tarjoaa SharePoint Server -tuotteen ominaisuudet ilman oman palvelininfrastruktuurin hankintaa ja ylläpitoa. SharePoint Onlinesta on olemassa kaksi eri versiota, joista käyttäjä voi valita tarvitsemansa version. Office 365:den pakettien yhteydessä mukana tuleva taso määräytyy Office 365:den palvelupaketin mukaisesti. [44]

SharePointin avulla voidaan yritykselle luoda muun muassa sisäinen intranet, yhteistyökumppaneille ekstranet, yrityksen kotisivut, työryhmätiloja omine kalentereineen ja sähköpostilaatikoineen, työnkulkuja ja metadatapohjaista dokumenttienhallintaa. SharePointin käyttötarkoitukset ovat moninaiset ja laajennettavissa tarpeiden mukaan.

3.2.3 LYNC ONLINE

Lync on Microsoftin pikaviesti- ja videoneuvotteluohjelmisto yritysasiakkaille. Lync Online on, samoin kuin SharePoint Online, Lync Server 2013 -palvelinversion pilvipalvelumalli. Se mahdollistaa lähes kaikki samat toiminnot kuin Server-versio. [45]

Lync Online sisältää yrityksen henkilöiden reaaliaikaiset tavoitettavuustiedot käytettävyystiedolla ja sijainnilla. Lyncin avulla voidaan järjestää kokouksia, se mahdollistaa video- ja äänipuhelut. Kokoukset voidaan määrittää helposti suoraan Outlook-kalenterin kautta myös yrityksen ulkopuolisten henkilöiden kanssa. Lisäksi sillä voidaan lähettää pikaviestejä ja jakaa työpöytäohjelmistojen näkymiä muille käyttäjille. [45]

3.2.4 ONEDRIVE FOR BUSINESS

OneDrive for Business on aiemmin SkyDrive Prona tunnettu yrityksen käyttäjien henkilökohtainen tallennustila. OneDrive for Business eroaa kuluttajapuolen OneDrivesta siten, että Business-versiossa yrityksellä säilyy hallinta yrityksen tietoihin ja palvelun kautta yrityksen järjestelmänvalvojat voivat määritellä esimerkiksi, voidaanko tietoja jakaa yrityksen ulkopuolelle. [46]

Oletuksena kaikki tiedostot OneDrive for Business -sovelluksessa ovat yksityisiä, ellei käyttäjä määritä tiedostoja jaetuiksi tai sijoita niitä yhteiseen kaikille jaettuun kansioon. Käyttäjä voi valita, mitkä kansiot tai tiedostot hän haluaa synkronoida offline-käyttöä varten. [46]

OneDrive for Business on synkronoitu yhteen Office 365 -portaalin ja SharePointin tiedostojärjestelmän kanssa. Esimerkiksi OneDrive for Business kansion, Shared with Everyone tiedostot ovat kaikkien yrityksen käyttäjien haettavissa yrityksen SharePointin kautta. OneDrive for Business -kansiossa sijaitsevat tiedostot käyttäytyvätkin kuten SharePoint-tiedostot. Käyttäjän tuleekin pohtia tiedostoja tallentaessaan, ovatko tiedostot tarpeellisia vain hänelle vai tulisiko tiedostojen olla suuremman ryhmän käytössä, jolloin tallennuspaikkana toimii paremmin jokin SharePointin ryhmätyötila. [46]

3.3 WINDOWS INTUNE

Microsoft julkaisi maaliskuussa 2011 Windows Intune -pilvipalvelun työasemien hallintaan. Palvelu mahdollistaa työasemien hallinnan riippumatta siitä, missä laitteet fyysisesti sijaitsevat – pelkkä internetyhteys riittää. Alun perin 11 euroa maksanut kuukausitilaus sisälsi hallinnan lisäksi mahdollisuuden käyttää tietokoneessa uusinta Windowsin käyttöjärjestelmäversiota ja Forefront-virustorjuntaa. Myöhemmissä julkaisuissa vaihtoehtoja tuli niin kuukausimaksun kuin sisällönkin suhteen useita lisää, ja nykyinen täyden version käyttäjäkohtainen perusmaksu on yhdeksän euroa kuukaudessa. Ensimmäisen perustoiminnot sisältäneen version jälkeen kehitys on ollut nopeaa, ja Intune kehittyy vauhdilla versio versiolta jatkuvasti lähemmäs nykyistä System Center Configuration Manageria (SCCM). Suurimpana erona System Centeriin tulee olemaan palvelun tarjonta pilvestä omien palvelimien sijaan. [47]

Intunen kohdalla päivitys tapahtuu automaattisesti aina uusimpaan versioon. Versioinnissa ei puhutakaan numeroista, vaan Intuneen on vakiintunut epävirallinen käytäntö puhua seuraavasta aallosta. Ensimmäinen versio oli nimetty Wave A:ksi, ja tällä hetkellä päivitykset ovat edenneet F-versioon saakka. Uuden version julkaisun jälkeen Intunen tiedotuskeskukseen tulee tieto ajankohdasta, jolloin versio tullaan päivittämään uuteen. Lisäksi koska Intunen hallintakonsolia käytetään internetselaimen kautta, ei käyttäjän tarvitse tehdä päivityksen suhteen mitään toimia. Työasemilla olevat client-ohjelmistot päivittävät myöskin itse itsensä versiopäivityksen yhteydessä.

Vuonna 2012 Microsoft muutti Intunen lisensointikäytäntöä vastaamaan paremmin nykyajan ympäristön vaatimuksia. Lisenssi muuttui laitekohtaisesta käyttäjäkohtaiseksi, ja nyt Intunen avulla voidaan hallita viittä eri päätelaitetta jokaista käyttäjää kohden. Intunen avulla voidaan hallita Windows-tietokoneiden lisäksi myös Mac OS -, Windows RT -, Windows Phone -, iOS- ja Android-laitteita. [48]

Windows Intune tekee paljon samoja asioita kuin SCCM, mutta näiden välillä on edelleen eroja. Paras kattavuus toimintoihin saadaankin SCCM:n ja Windows Intunen yhdistelmällä (taulukko 6).

Taulukko 6. Windows Intunen vertailua System Center 2012 R2 Configuration Manageriin. [49]

Tapaus	System Center 2012 R2 Configuration Manager	Windows Intune	System Center 2012 R2 Configuration Manager ja Windows Intune
Eri alustoiden tuki			
Microsoft Windows	Kyllä	Kyllä	Kyllä
Microsoft Windows Server	Kyllä	Ei	Kyllä
Windows Phone	Ei	Kyllä	Kyllä
Windows RT	Ei	Kyllä	Kyllä
iOS	Ei	Kyllä	Kyllä
Android	Ei	Kyllä	Kyllä
Mac OS X	Kyllä	Ei	Kyllä
Unix/Linux Servers	Kyllä	Ei	Kyllä
Asetusten valvonta			
Laajat Windows-koneiden asetusten konfigurointimahdollisuudet (mm. WMI, rekisteri)	Kyllä	Ei	Kyllä
Laajat Mac OS X -koneiden asetusten konfigurointi	Kyllä	Ei	Kyllä
Mobiililaitteiden asetusten konfigurointi	Ei	Kyllä	Kyllä
Jakelu			
Sovellusten jakelu	Kyllä	Kyllä	Kyllä
Windows-käyttöjärjestelmän jakelu	Kyllä	Ei	Kyllä
Turvallisuus ja yksityisyys			
Ohjelmistojen päivitykset	Kyllä	Kyllä	Kyllä
Endpoint Protection	Kyllä	Kyllä	Kyllä
Hallinta ja raportointi			
Sovellusten monitorointi	Kyllä	Ei	Kyllä
Laitteiston ja sovellusten inventointi	Kyllä	Kyllä	Kyllä
Kustomoidut laite- ja sovelluskannan inventointi	Kyllä	Ei	Kyllä
Roolipohjainen järjestelmänhallinta ja raportointi	Kyllä	Ei	Kyllä
Yhdistetty raportointi pilvi- ja oman konesalin palveluista	Ei	Ei	Kyllä
Pilvipohjainen raportointi	Ei	Kyllä	Ei
Mobiililaitteiden datan suojaaminen			
Turvallisuusasetukset	Kyllä	Kyllä	Kyllä
Etätyhjennys	Kyllä	Kyllä	Kyllä
Etälukitus	Ei	Kyllä	Ei
Turvakoodin nollaus	Ei	Kyllä	Ei

Kuten taulukosta 6 nähdään, laajimpaan hallintaan päästään Intunen ja System Centerin yhdistelmällä. Mobiililaitteiden hallinnassa Intunen pilviominaisuudet tulevat parhaiten esiin. Mobiililaitteiden hallinta koetaankin Microsoftilla erittäin tärkeäksi, ja tämä osio on Intunen eniten kehittyvä osio tulevissa julkaisuissa. [50]

Laitehallinnan lisäksi Intunen lisenssi antaa yritykselle uusia mahdollisuuksia tietoturvansa parantamiseen. Intunen täysversion lisenssin mahdollistamien Windows Enterprise -versioiden käyttäminen tuo mukanaan joitakin vain suurempien yritysten käytössä olevia turvaominaisuuksia. Näistä tärkein ominaisuus lienee BitLocker, jolla voidaan pakottaa levytilan salaus päälle käyttäjän koneessa ja tarvittaessa myös muistitikuilla. Tällöin kadonneen muistitikun tai tietokoneen tietoja ei pystytä lukemaan. Muita mahdollisesti hyödyllisiä ominaisuuksia ovat AppLocker, jolla voidaan määritellä hyväksyttävät ohjelmistot, DirectAccess-tekniikka VPN-yhteyksien korvaajaksi sekä BranchCache-välimuistipalvelu. [51]

3.4 LUOTTAMUS MICROSOFTIN PILVITOIMINTAMALLISSA

Kuten tässä diplomityössä luottamusta käsittelevässä osiossa todettiin, pilvipalveluiden olemassaolo riippuu käyttäjistä ja lopulta heidän luottamuksestaan palveluun. Myös Microsoft ottaa tosissaan luottamuksen rakentamisen tuotteitansa kohtaan. Joulukuussa 2011 julkaistussa Privacy in the Public Cloud: The Office 365 Approach -esitteessä Microsoft uskoo julkisten pilvipalveluiden olevan lähitulevaisuuden suosituin pilvipalvelumalli. Kuitenkin he samalla toteavat, että julkisen pilven kasvu ei ole väistämätöntä vaan heidän täytyy kyetä vastaamaan käyttäjien kysymyksiin ja vaateisiin datan suojaamiseksi, jotta tarvittava luottamus palveluita kohtaan voidaan ansaita. [52]

Näistä kasvun mahdollisista uhkakuvista pilvitoimintamallin yritykset saivat NSA:n vakoiluskandaalin kautta esimerkin, jonka vaikutukset tuntuvat vielä pitkään. Myös Microsoft on joutunut NSA-vakoilun kohteeksi. Vuotaneista tiedoista ei ole tarkalleen selvinnyt, mihin kaikkialle NSA:lla on ollut pääsy, mutta pelkkä epäilys on vaikuttanut Microsoftin toimintaan. Tämän johdosta yritys on ryhtynyt mittaviin toimenpiteisiin lisätäkseen luottamusta käyttäjien datan suojaamiseksi.

Salauksen lisääminen läpi palvelujen on yksi konkreettinen esimerkki tapahtuneista muutoksista. [53]

Microsoft onkin tehnyt paljon toimia tuon vuonna 2011 kirjoitetun lausunnon jälkeen. Uusimmassa ”Security and Compliance, Office 365” teknisessä raportissa toukokuulta 2014, Microsoft käy läpi useita palveluun jo tulleita uusia ominaisuuksia sekä seuraavassa versiossa julkaistavia turvallisuuspäivityksiä. Microsoft toteaa dokumentissaan Office 365:den turvallisuuden kehittymisen olevan jatkuva prosessi, jota ylläpidetään ja kehitetään parhaiden resurssien avulla [54]. Esimerkiksi Office 365:den parissa työskentelee useita satoja tietotekniikan ammattilaisia, jotka huolehtivat pelkästään järjestelmän tietoturva-asioiden oikeanlaisesta toteutuksesta. Onkin melko selvää, että pk-yrityksen omien palvelinten toteutuksissa ei päästä samalle tasolle palvelujen ominaisuuksien ja saavutettavuuden suhteen. Saavutettavuudessa esimerkiksi Microsoft lupaa 99,9 % tason, mutta käytännössä toteutunut taso on ollut 99,94 – 99,99 % välillä (taulukko 7) [55]. Vaikka lukemina molemmat tuntuvat suurilta, on viimeisen yhdeksikön merkitys suuri pohdittaessa mahdollisia käyttökatkoja. 99,9 %:n tasolla voi kuukaudessa olla yhteensä käyttökatkoa lähes 44 minuuttia, kun taas 99,99 %:n tasolla kuukausittainen käyttökatko on vain hieman päälle 4 minuuttia.

Taulukko 7. Microsoftin julkaisemat neljännesvuosittaiset käytettävyysajat Office 365 -palvelulle. [55]

2012		2013				2014
99.98%	99.97%	99.94%	99.97%	99.96%	99.98%	99.99%
Q3	Q4	Q1	Q2	Q3	Q4	Q1

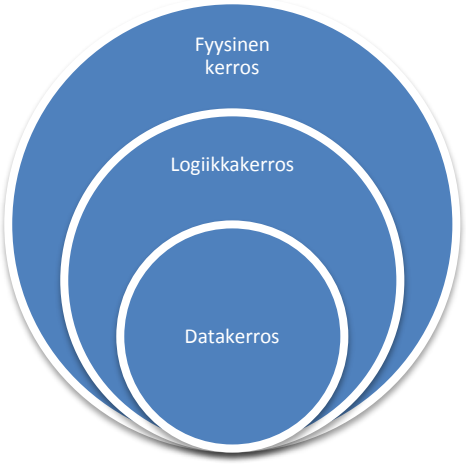
Microsoft kertoo asiakkailleen palveluidensa reaaliaikaisen statuksen. Muille kuin asiakkaille on sivustolla http://www.trustoffice365.com tarjolla neljännesvuosittain kooste käytettävyysajasta. Kyseinen luottamussivusto sisältää on paljon muutakin tietoa, jolla Microsoft pyrkii lisäämään palvelujensa läpinäkyvyyttä kuluttajille. Vastaavia sivustoja on olemassa myös muilla pilvipalveluita tarjoavilla yrityksillä,

esimerkiksi Google kertoo palveluidensa toiminnasta osoitteessa http://www.google.com/appsstatus ja Salesforce osoitteessa http://trust.salesforce.com/trust/.

Microsoftin toimet tietoturvan, määräystenmukaisuuden ja yksityisyyden takaamiseksi jakavat asiat kahteen pääosioon: palveluissa itsessään oleviin turvatekijöihin sekä käyttäjän hallinnoimiin ominaisuuksiin. [54]

3.4.1 PILVIPALVELUIDEN SISÄÄNRAKENNETUT TURVAOMINAISUUDET

Microsoftilla on vuosien kokemus yritystason ratkaisujen ja Online-palvelujen toteutuksesta, ja toteutusten on tarkoitus täyttää kaikki alan tiukat määräystenmukaisuusstandardit. Microsoft jakaa sisäänrakennetut suojaominaisuudet kuvan 12 mukaisesti usealle tasolle. Suojauksen jakaminen omille kerroksilleen takaa Microsoftin mukaan suojauksen toteutumisen myös tilanteessa, jossa jonkin kerroksen suojaus on pettänyt. [54]



Kuva 12. Microsoft on rakentanut suojauksensa erillisille sisäkkäisille suojaustasoille Office 365 -palvelussa. [54]

Fyysisen kerroksen suojaus sisältää palvelinsalien ja verkon suojaamisen. Fyysiset palvelinkeskukset ovat tiukasti valvotut ympäri vuorokauden, ja ne ovat suojattuja

niin luonnonilmiöiltä kuin myös fyysiseltä pääsyltään [54]. Office 365 Trust Center tiivistää fyysisen kerroksen suojaamisen seuraaviin kohtiin:

- Ympärivuorokautinen palvelinkeskusten valvonta
- Palvelinsaliin pääsy edellyttää monivaiheisen tunnistamisen biometrisine tunnisteineen
- Palvelinkeskuksen sisäisen verkon eristäminen ulkoisesta verkosta
- Roolipohjainen tiedon eristäminen sotkee datan tunnistamattomaan muotoon, joten fyysisen pääsyn omaavat henkilöt eivät pysty tietoja lukemaan
- Vialliset tallennusasemat ja laitteisto tuhotaan ja demagnetisoidaan

[55]

Logiikkakerros sisältää prosesseja ja hallintaominaisuuksia, joilla suojataan isäntäkone, isäntäkoneella ajettavat sovellukset sekä näiden molempien suojaaminen järjestelmänvalvojien mahdollisesti haitallisilta toimilta. Prosessit pyritään automatisoimaan, jotta tarve ihmisten tekemille toimille järjestelmän sisällä jäisi mahdollisimman vähiin. [54]. Office 365 Trust Center kuvaa logiikkakerroksen toimet seuraavilla kohdilla:

- ”Lock box” -prosessi valvoo tiukasti järjestelmänvalvojien pääsyä dataan
- Palvelimet suorittavat vain prosesseja, jotka ovat hyväksytyllä whitelist-luettelolla ja näin minimoidaan haitallisen koodin suorittamisen riski
- Uhkakuvien hallintaan erikoistuneet tiimit varautuvat ennakoivasti estääkseen haitallisen toiminnan pääsyn järjestelmiin
- Porttiskannaukset, järjestelmän ulkoreunan haavoittuvaisuuksien skannaukset sekä tunkeilijan havaitsemisjärjestelmät estävät tai havaitsevat kaiken haitallisen pääsyn järjestelmiin

[55]

Datakerroksen suojauksessa ensimmäinen tekijä, johtuen pilvipalvelun usean käyttäjän ympäristöstä, on jaettujen resurssien käytössä datan eristäminen muiden käyttäjien datasta. Tämä eristäminen tapahtuu Active Directoryn tähän tarkoitukseen

suunniteltujen työkalujen avulla [54]. Muun suojauksen datakerroksella Office 365 Trust Center tiivistää seuraavasti:

- Palvelimilla oleva data on suojattu kryptauksella
- Siirrettäessä data suojataan SSL/TLS-salauksella
- Uhkakuvien hallinta, tietoturvan monitorointi ja tiedostojen/datan eheys estävät tai havaitsevat kaikki yritykset datan luvattomasta käsittelystä

[55]

Tarkempia kuvauksia Microsoftin käyttämistä suojaustoimista löytyy http://www.trustoffice365.com sivustolta. Lupauksien kirjoittamista tärkeämpinä tekijänä luottamuksen muodostumisessa pilvipalveluiden tapauksessa on kuitenkin riippumattomien kolmansien osapuolien sertifikaatit ja standardit, joilla yritys pystyy todistamaan toimivansa samoin niin kuin ilmoittavat.

Tärkeimpinä näyttöinä luottamuksen rakentamiseksi Office 365 -palveluihin Microsoft nimeää ISO 27001 -auditoinnin ja -sertifioinnin, SSA 16 SOC1 Type II –todistuksen sekä HIPAA-sopimuksen ehtojen ja vaatimusten täyttämisen. [54]

3.4.2 KÄYTTÄJÄN HALLINNOIMAT TURVAOMINAISUUDET

Pilvitoimintamallin sisäänrakennettuihin ominaisuuksiin käyttäjä ei voi vaikuttaa. Office 365:den hallintaominaisuudet mahdollistavat Exchange Onlinen, SharePoint Onlinen ja Lync Onlinen osalta yksilöllisiä turvaominaisuuksia, joita yrityksen pääkäyttäjä voi määritellä. Näiden avulla käyttäjä voi täyttää yrityksen sisäiset vaatimukset, määritellä pääsyn palveluihin ja sisältöön ja määritellä haittaohjelma- ja roskapostisääntöjä, sekä uusimpana ominaisuutena määritellä datan salauksen sääntöjä. [54]

Käyttäjän hallinnoimista työkaluista on syytä nostaa esiin muutama uusi ominaisuus. Multi-Factor Authentication (MFA), eli monivaiheinen todentaminen, on ollut jo pidempään mahdollista kytkeä Office 365:ssä päälle järjestelmänvalvojien tileille. Helmikuussa 2014 MFA:n käyttö tuli mahdolliseksi kaikilla Office 365:den

tileillä käytettäessä sovelluksia internetselaimen välityksellä. MFA käyttää Azuren Multi-Factor Authentication -palvelua todennuksen toteuttamiseen. [56]

MFA-todennuksessa käyttäjän kirjautuessa internetsivun kautta palveluihin sisään omilla Office 365 -tunnuksillaan, lähetetään käyttäjälle puhelimeen tekstiviestinä kuusinumeroinen koodi, joka pitää lisävarmistuksena antaa kirjautumissivustolle. MFA mahdollistaa myös puhelimella Multi-Factor-sovelluksen käytön, joka tunnistaa käyttäjän kirjautumisyrityksen. Sovelluksen kautta palvelua käytettäessä riittää, kun käyttäjä joko hyväksyy tai hylkää kirjauksen sovelluksessa. Sovelluksesta voi myös suoraan raportoida järjestelmänvalvojalle luvattomista kirjautumisyrityksistä. [56]

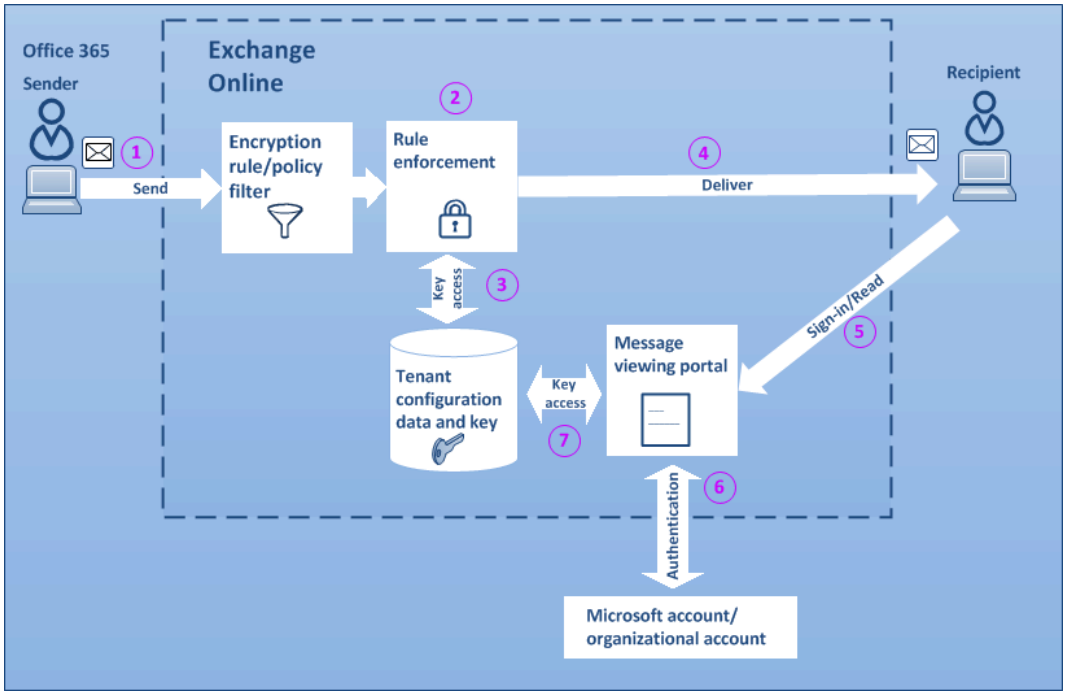
Salaus ja tiedon suojaus kuuluu suurelta osin käyttäjän hallinnoimiin ominaisuuksiin, mutta kokonaiskuvan vuoksi listattuna on myös järjestelmän sisäiset salauksenkäytön menetelmät. Office 365 käyttää eri salaustekniikoita tiedonsiirron ja säilytyksen eri vaiheissa:

- TLS (Transport Layer Security) salaa tiedonsiirtoyhteyden sähköpostipalvelimien välillä. Tällä salauksella estetään, etteivät verkon salakuunteluyritykset pääse käsiksi siirrettävään tietoon.
- SSL (Secure Socket Layer) -salausta käytetään sähköpostiohjelmistojen ja Office 365 -palvelinten muodostaessa yhteyden.
- BitLocker-salausta käytetään datakeskusten tallennustilan salaamiseen. Tällä estetään muiden kuin käyttöoikeuden omaavien pääsy dataan.
- IRM (Information Rights Management) -sisältöoikeuksien hallintaan Office 365 käyttää Windows Azure Rights Management -palvelua. Sisältöoikeuksien hallinnalla saadaan yrityksen kriittinen tieto halutessa suojattua tulostamiselta, edelleen lähettämiseltä tai luvattomalta kopioinnilta sekä määritettyä tiedolle voimassaoloaika, jolloin tieto on luettavissa. IRM-suojauksen asetukset säilyvät, vaikka tiedosto olisi siirretty muistitikulle tai muualle offline-tilaan.
- S/MIME (Secure/Multipurpose Internet Mail Extensions) -sähköpostiviestien salausmahdollisuus.

  [57]

Yhtenä uusimmista käyttäjien tietoturvaa parantavista ominaisuuksista Microsoft julkaisi huhtikuun 2014 alussa Office 365 Message Encryption (OME) -palvelun. Se on rakennettu Azuren Rights Management (Azure RMS) -palvelun päälle, ja se on otettavissa suuryritysten Office 365 -paketteihin käyttöön ilmaiseksi. Verrattuna S/MIME-salaustekniikan käyttöön OME on hallinnallisesti huomattavasti helpompi ottaa yrityksessä käyttöön, ja sen kautta voidaan lähettää salattuja viestejä kenelle tahansa vastaanottajalle. [58]

Office 365 Message Encryption on verkkopalvelu, joka toimii Azure RMS:n avulla. Kuvassa 13 on esitetty salatun viestin lähettäminen ja vastaanottaminen. Järjestelmänvalvojat voivat luoda haluttuja sääntöjä viestin sisällön, lähettäjän tai vastaanottajan mukaisesti. Jos sääntö toteutuu, viesti salataan ja tieto vastaanotetusta salatusta viestistä lähetetään vastaanottajalle. Lukeakseen viestin vastaanottajan täytyy tunnistautua viestin lukuportaaliin. Tunnistautuminen portaaliin tapahtuu Microsofttunnuksilla, joten jos kyseiselle sähköpostitunnukselle ei ole olemassa vastaavaa Microsoft-tiliä tai -organisaatiotunnusta, sellainen pitää ensimmäisellä kerralla luoda. Vahvistuksen jälkeen salaus puretaan organisaation salausavaimella, joka sijaitsee ennalta määritetyssä sijainnissa eikä lähettäjän eikä vastaanottajan tarvitse tietää mitään avainkäytännöistä. [58]



Kuva 13. Kaaviokuva Office 365 -viestien online-salauksesta, jolla sähköpostiviestien salaaminen voidaan toteuttaa kenen tahansa vastaanottajan kanssa. Salattujen viestien lukeminen tapahtuu erillisen portaalin kautta. [58]

Myös OneDrive for Business - ja SharePoint Online -palvelujen sisältö muuttuu levykohtaisesta salauksesta tiedostokohtaiseen salaukseen. Tämä muutos tuli Office 365 -palveluun heinäkuussa 2014. Muutoksen jälkeen jokainen tiedosto SharePoint-palvelussa ja OneDrive for Business -palvelussa kryptataan omalla avaimellaan. Lisäksi organisaation tiedostot hajautetaan useiden Microsoft Azuren tallennustilojen kesken. Tämä ja tiedostojen sekä tiedostojen sijainnin kartan kryptaaminen parantavat huomattavasti tiedostotilojen turvallisuutta. [54]

4 TUTKIMUKSEN TOTEUTUS TESTIYMPÄRISTÖN AVULLA

Kohdeyrityksellä on ollut Microsoftin pilvipalveluita käytössä lähes niiden ensijulkaisusta asti. Ajansaatossa palveluihin on tullut paljon muutoksia ja uusia ominaisuuksia, joita ei ole yrityksessä hyödynnetty lähinnä ajan puutteen ja resurssien niukkuuden vuoksi. Tämän takia yrityksen johdon ja IT-henkilöiden kesken tehtiin vaatimusmäärittely, jonka pohjalta työssä alettiin tutkia pilvipalveluiden tämänhetkisten ominaisuuksien soveltuvuutta yrityksen tarpeisiin ja mitä ominaisuuksia palveluista kannattaa yrityksessä ottaa käyttöön. Vaatimusmäärittely on liitteessä 1.

Työssä tehtiin yrityksen oman IT-ympäristön lisäksi tutkimusympäristö, jossa ominaisuuksia pystyttiin tutkimaan ilman yritysympäristön vaarantamista. Lisäksi tutkimusympäristössä päästiin todenmukaiseen tilanteeseen, jossa Office 365 ja Windows Intune toimivat samoilla tunnuksilla, ja näin ollen Intunen kaikki hallintaominaisuudet saatiin käyttöön.

Yrityksen tekemän vaatimusmäärittelyn kohdat jaettiin Windows Intunen ja Office 365:den välillä. Joihinkin vaateisiin pystytään vastaamaan molempien pilvipalveluiden ominaisuuksilla tai näiden yhdistelmillä. Lisäksi mukaan otettiin palveluiden laajentaminen Microsoft Azure ympäristöön.

4.1 TUTKIMUSYMPÄRISTÖN LAITTEET JA OHJELMISTOT

Tutkimusympäristö koottiin yrityksen käytöstä poistuneiden PC-tietokoneiden avulla. Mobiililaitteina käytettiin sekä yrityksen laitteita että henkilökohtaisessa käytössä olevia laitteita. Yrityksen pääalustana mobiilipuolella on pääosin Windows Phone, mutta testiin saatiin myös Android-puhelin sekä iOS iPadin muodossa. IPadin lisäksi tutkimusympäristöön saatiin mukaan myös Windows RT -tabletti.

Tietokoneet asennettiin uudestaan ja käyttöön otettiin joko Windows 7 Enterprise - tai Windows 8.1 Enterprise - versiot, jotka vastaavat yrityksessä käytettäviä käyt-

töjärjestelmiä. Windows Intune -asiakasohjelmisto asennettiin jokaiseen tietokoneeseen hallintasovellukseksi. Intunen kautta tietokoneisiin asentui ajantasainen virustorjunta- ja palomuurisovellus, Endpoint Protection, sekä käyttöjärjestelmälisenssit, jotka sisältyvät Windows Intunen kuukausimaksuun.

Toimistosovelluksien osalta osaan tietokoneista asennettiin Office 365:den mukana tulevien Office ohjelmien uusimmat työpöytäversiot ja osassa testattiin sovellusten verkkokäyttöä selaimen kautta sekä Office on Demand -palvelun avulla.

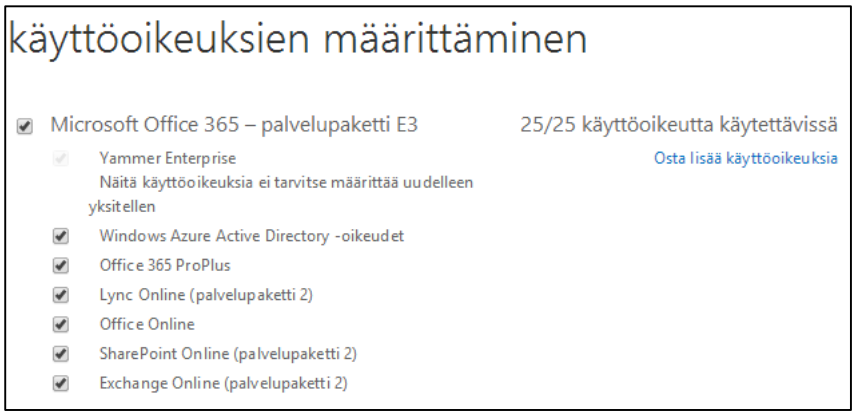
4.2 MICROSOFTIN PILVIPALVELUIDEN KÄYTTÖÖNOTTO

Testiympäristön luonti aloitettiin luomalla testitunnukset Windows Intune -palveluun. Tämä onnistui nopeasti Microsoftin Intune -sivujen kautta. Kokeiluversion myötä testikäyttöön saatiin 25 käyttöoikeutta 30 vuorokauden ajaksi. Kirjautumistunnuksia tehtäessä ympäristölle täytyi määrittää uusi vapaana oleva toimialueen nimi ”.onmicrosoft.com” -päätteiselle osoitteelle. Jos yrityksellä on jo oma rekisteröity toimialueen nimi, se voidaan yhdistää Microsoftin palveluihin myöhemmin.

Office 365:den käyttöönotto tapahtui hyvin samalla tavalla kuin Windows Intunen. Ainoana erona kirjautumisessa on, että nyt palveluun kirjaudutaan aiemmin Intunen avauksen yhteydessä luoduilla testitunnuksilla. Täten palvelut toimivat yhdessä kuten niiden on ajateltukin. Kokeiluversioksi valittiin ominaisuuksien takia E3-taso. E3 on myös laajimmin käytössä oleva lisenssitaso kohdeyrityksessä. Koekäyttö sisältää 25 lisenssiä, joilla päästään tutustumaan kaikkiin Office 365:den palveluihin 30 vuorokauden ajan.

Käyttäjien luonti, muokkaaminen ja poisto voidaan tehdä joko Windows Intunen tai Office 365:den puolelta. Työssä käyttäjät 1-4 luotiin suoraan Office 365:den puolen aloitusnäkymän ”siirry käyttäjiin ja ryhmiin” -linkin kautta. Palveluiden käyttäjätietokantojen yhteen toimivuuden testaamiseksi, luotiin viides käyttäjä Intunen puolelta ja todettiin käyttäjätietojen ilmaantuvan välittömästi myös Office 365:den aktiivisiin käyttäjiin. Käyttäjille tulee erikseen määrittää molemmissa palveluissa palvelut, joihin heillä on käyttöoikeus. Esimerkiksi jos käyttäjätili on luotu

Windows Intunen kautta, tulee Office 365:ssä valita halutut käyttöoikeudet (kuva 14) ja vastaavasti Office 365:den kautta luoduille käyttäjätileille tulee valita halutut käyttöoikeudet Windows Intunessa.



Kuva 14. Office 365 E3 -palvelupaketin sisältö. Tarvittaessa palveluita voidaan karsia käyttäjäkohtaisesti myös palvelupakettien sisällä.

Samoilla testitunnuksilla testiympäristöä laajennettiin myös Microsoft Azuren puolelle. Azuren koekäyttö sisältää ilmaisia krediittejä 150 euron edestä 30 vuorokauden aikana. Azureen kirjautuminen on luonteva jatke Intunen ja Office 365:den lisäksi, sillä molemmat käyttävät taustalla Azuren tekniikkaa ja käyttäjätietokanta sijaitsee valmiiksi Windows Azure Active Directory, WAAD, -palvelussa.

Peruspalveluiden luomisen jälkeen aloitettiin tutkimaan palveluiden ominaisuuksia kohdeyrityksen näkökulmasta. Office 365:dessä ja Windows Intunessa on paljon ominaisuuksia, joten niiden kaikkien läpikäyminen ei ole tässä työssä mahdollista. Tutkimuksessa tehtiinkin oletus, että palveluissa alusta asti mukana olleet perusominaisuudet ovat jo yrityksellä käytössä, joten näiden ominaisuuksien uudelleen läpikäynti ei tuo tälle työlle lisäarvoa. Tehdyn oletuksen perusteella tutkimus painotettiin enimmäkseen palveluihin tulleisiin uusiin ominaisuuksiin, joista olisi hyötyä yrityksen tietoturvan ja hallinnan kehittämisen kannalta.

4.3 WINDOWS INTUNE TESTIYMPÄRISTÖSSÄ

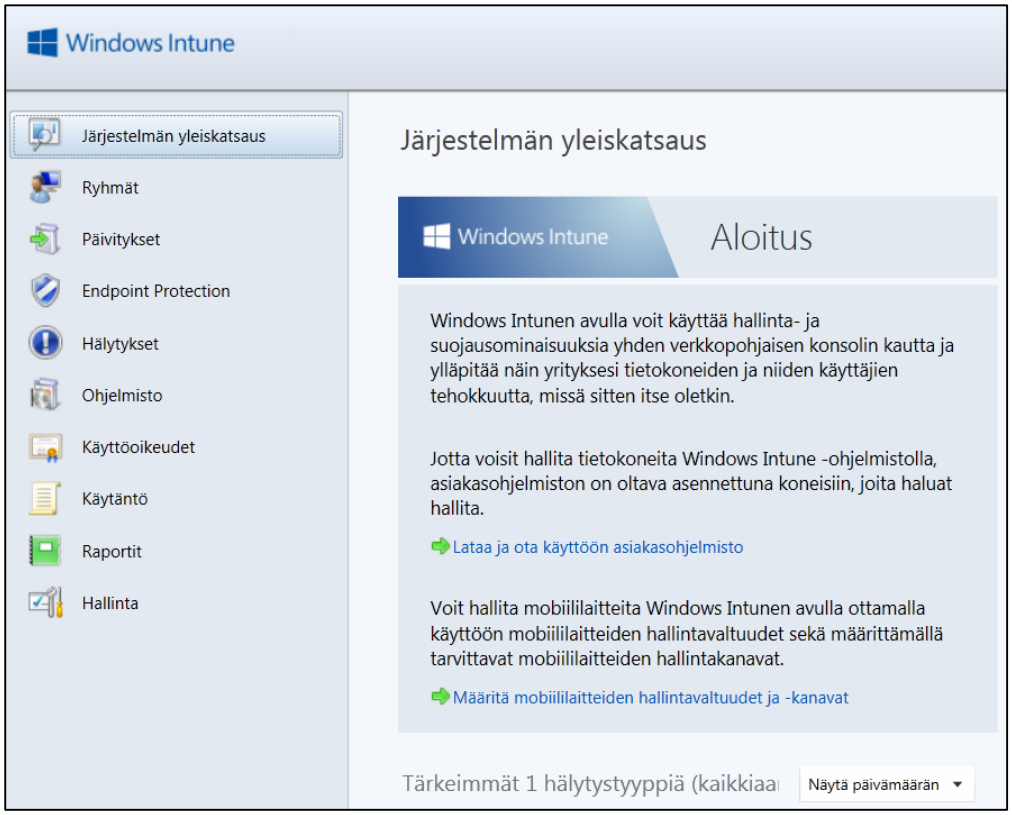
Kuten teoriaosuudessa todettiin, Windows Intune toimii päätelaitehallinnan alustana, joka tarjoaa laajan tuen eri alustoille. Intunen avulla voidaan määritellä ja valvoa päätelaitteiden asetuksia, käyttää keskitettyä Endpoint Protection -virustorjuntaa, jakaa ja päivittää ohjelmistoja, inventoida laite- ja sovelluskanta, tehdä erinäisiä raportteja sekä toteuttaa mobiililaitteiden datan suojausta.

Yrityksen tekemän vaatimusmäärittelyn mukaisista asioista Windows Intunea koskettivat vaateet: 1, 2, 3, 4, 7, 8, 10 ja 11. Nämä vaatimukset voidaan jakaa päätelaitteiden hallintaan (kohdat 1 ja 4), ohjelmistoversioiden ja lisenssien hallintaan (kohdat 2 ja 3), etänä tehtäviin toimenpiteisiin (kohdat 8, 10 ja 11) sekä tietoturvasäännöstöihin ja valvontaan (kohta 7). Kyseiset vaatimukset on esitetty koostettuna taulukossa 7.

Taulukko 8. Vaatimukset, joihin etsittiin vastauksia Windows Intunen avulla

Nro	Vaatimus	Yhteinen tekijä
1	Kaikkien tietokoneiden hallinta riippumatta sijainnista	Päätelaitehallinta
4	Mobiililaitteiden hallinta	
2	Tiedot asennetuista ohjelmistoista	Asennetut ohjelmistot
3	Lisenssien hallinta	
8	Etätoimet laitteille	Etätoimet
10	Etätuki	
11	Ohjelmistojen ja päivitysten asennukset	
7	Tietoturvamääritykset ja valvonta	Tietoturva
5	*Käyttäjän tiedostot käytettävissä kaikilla päätelaitteilla*	
6	*Yrityksen yhteiset tiedostot saavutettavissa kaikilla päätelaitteilla*	
12	*Yrityksen datan suojaaminen*	
13	*Projektien tiedostojen jako ja arkistointi*	
14	*Yhdet kirjautumistunnukset*	
15	*Turvallinen sähköpostiliikenne*	
16	*Kadonneen salasanan hyödyntämisen havaitseminen*	
17	*Yhteysongelmatilanteissa toiminnan jatkuminen*	

Windows Intunen määrittely aloitettiin käyttäjätilien luomisen jälkeen lataamalla hallintakonsolista (kuva 15) tietokoneille asiakasohjelmisto. Ennen asiakasohjelmiston lataamista Intune pyytää tekemään Windows Intune Agent -käytännön, jolla määritellään muun muassa Endpoint Protection -asennus sekä automaattisen haittaohjelmien tarkistuksen käytännöt.



Kuva 15. Ruutukaappaus Windows Intunen hallintakonsolin aloitusnäkymästä.

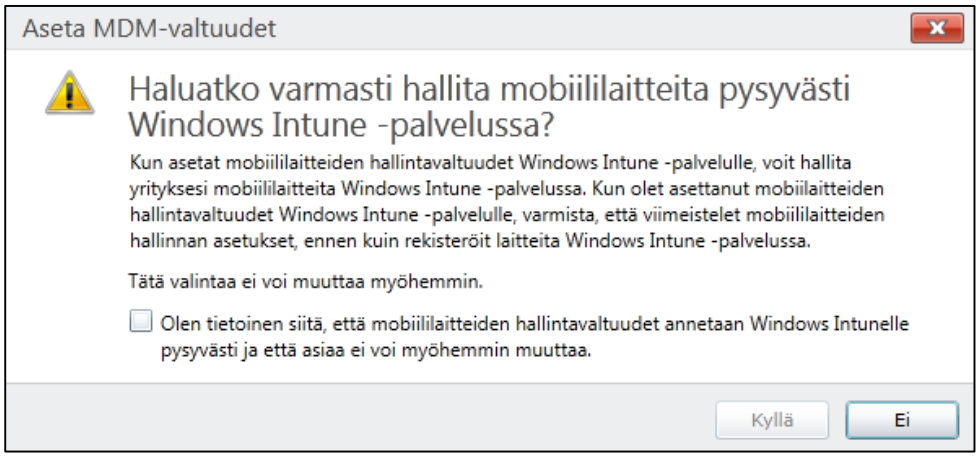
Testiympäristööni luotiin alkuun kaksi organisaatioryhmää: toimisto ja työmaat. Ryhmille voidaan valita käyttäjät yksitellen, sääntöjen perusteella tai Office 365:den puolella määriteltyjen käyttöoikeusryhmien perusteella. Testiympäristössä tehtiin ensin Office 365:den hallintakonsolissa käyttöoikeusryhmät toimistotyöntekijöille ja työmaahenkilöille. Ryhmien määrityksen jälkeen ne olivat heti käytettävissä myös Windows Intunen puolella.

Yrityksen vaatimuksista ensimmäinen, vaatimus tietokoneiden hallinnasta riippumatta laitesijainnista, on ollut Windows Intunen perusominaisuus ensijulkaisusta asti, ja tämä osio on kohdeyrityksessä jo toteutettu asianmukaisesti. Uudempi ominaisuus Intunen osalta on mobiililaitteiden hallinta, joka nykyisin on osin pakon sanelemana toteutettu yrityksessä Mail for Exchange -tekniikalla. Olikin syytä tutkia, mitä uusia mahdollisuuksia Windows Intunen mobiililaitehallinta voisi tuoda yrityksen laitehallintaan.

4.3.1 WINDOWS INTUNEN MOBILE DEVICE MANAGEMENT

Mobiililaitteiden tehokas hallinta on joidenkin alustojen kohdalla tähän asti vaatinut hybridiympäristön rakentamisen, jossa Windows Intunen rinnalla on käytössä Microsoftin Configuration Manager talon sisäisenä ratkaisuna. Microsoft on kuitenkin ottanut tavoitteekseen MDM-ominaisuuksien parantamisen pelkästään Windows Intune –pilvipalvelutoteutuksessa. Tämän vuoden aikana onkin tullut jo kaksi päivitystä, jotka ovat parantaneet ominaisuuksia merkittävästi.

Mobiililaitteiden hallinnan käyttöönottamiseksi Windows Intunen puolella täytyi tehdä muutamia toimia, joiden tekemiseksi Intunesta löytyi valmiit linkit ja ohjeet. Ensin mobiililaitteiden hallintavaltuudet (MDM, Mobile Device Management) täytyi määrittää Windows Intunelle (kuva 16). Tällä määrityksellä tehdään päätös mobiililaitteiden hallitsemisesta Windows Intunen kautta.



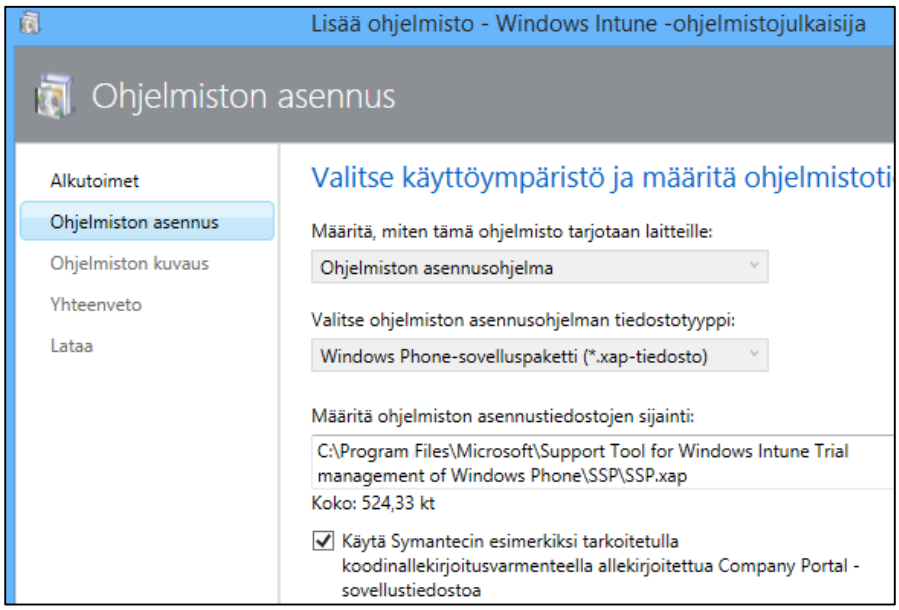
Kuva 16. MDM-valtuuksien asettaminen Windows Intunelle siirtää hallinnan pysyvästi Windows Intunen puolelle.

MDM-valtuuksien antamisen jälkeen täytyi määrittää jokaiselle mobiililaitekäyttöjärjestelmälle erikseen suora hallinta. Tällä hetkellä Intunen mobiililaitehallinnalla voidaan hallita Android-, Windows Phone -, Windows RT - sekä iOS-käyttöjärjestelmän laitteita.

Android-laitteiden kohdalla hallinnan aloittaminen oli kaikkein helpointa, koska erillisiä sertifikaatteja tai avaimia ei tarvitse asentaa. Googlen Play-kaupasta ladattiin Windows Intune -yritysportaalisovellus Android-puhelimeen. Sovellus kysyi käynnistyttyään käyttäjän yritystunnuksia, minkä jälkeen laite piti vielä hyväksyä lisättäväksi yritysportaaliin. Tämän jälkeen laite näkyy Intunen laitehallinnassa.

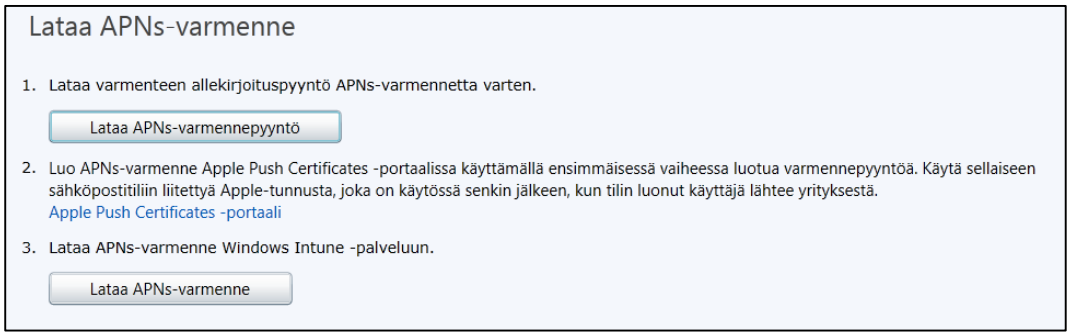
Windows Phone 8:n kohdalla testiympäristön toiminnan tutkiminen oli huomattavasti vaikeampaa. Windows Phonen hallinnan käyttöönotto tarvitsee ensin rekisteröintipalvelimen osoitteen, joka voidaan asettaa DNS-tietueella automaattisesti tai jonka käyttäjä voi asettaa asennuksen aikana. Testiympäristössä valittiin jälkimmäisen vaihtoehdon, jolloin osoitteeksi tulee laittaa enterpriseenrollment-s.manage.microsoft.com. Käyttöönoton seuraavassa vaiheessa tulisi hankkia käyttäjille jaettava yritysportaalisovellus, joka tulee olla allekirjoitettu koodinallekirjoitusvarmenteella. Tämän varmenteen voi hankkia Symantecin kautta, mutta koska kyseessä on maksullinen palvelu ilman koeaikaa, tämä vaihe ei tullut testiympäristössä kyseeseen. Tämän ongelman ratkaisemiseksi Microsoft julkaisi huhtikuussa

2014 työkalun, Support tool for Windows Phone trial management (kuva 17). Tämän työkalun avulla voidaan MDM-hallinnan testi suorittaa myös Windows Phonen kanssa.



Kuva 17. Support Tool for Windows Phone trial management -lisäosan asentaminen testiympäristöön korvaa maksullisen Symantecin koodinallekirjoitusvarmenteen.

iOS-mobiilikäyttöjärjestelmien kohdalla toimet aloitetaan lähettämällä varmennepyyntö Applen Push Certificates Portaliin (APNs-varmenne). Intunesta ladattu varmennepyyntö (kuva 18) vietiin Apple Push Certificates – portaaliin. Tämän jälkeen portaalista voitiin ladata itse APNs-varmenne, ja tämä varmenne tuotiin takaisin Intuneen. Varmenteen tuonnin jälkeen iOS-laitteet saadaan MDM-hallinnan piiriin.



Kuva 18. iOS-mobiilikäyttöjärjestelmän tarvitsemat toimet APNs-varmenteen hankkimiseksi jakautuvat kolmeen osaan: varmennepyynnön lataamiseen Intunesta, itse varmenteen luontiin Applen palvelussa ja varmenteen tuomiseen Intuneen.

Windows RT -käyttöjärjestelmän hallintaan liittämistä varten ei ole erillisiä vaatimuksia. RT:n sovelluksien hallintaa varten tarvitaan latausavain sekä koodinallekirjoitusvarmenne, jolla jaettavat ohjelmistot allekirjoitetaan. Testiympäristössä luotiin latausavain ja jaettiin RT-tabletille ohjelmistoja suoraan Windows-kaupasta linkillä, samoin kuin muiden käyttöjärjestelmien kohdalla. Tämän jälkeen asennettavissa olevat ohjelmistot tulivat näkyviin yritysportaaliin. RT:n suhteen vaatimukset koskevat siis lähinnä omien ohjelmistojen jakelua. Suorilla linkeillä pystytään käyttäjälle tarjoamaan yrityksen suosimia ohjelmistoja suoraan Windows-kaupasta. Myös Windows 8 - ja 8.1 - laitteita voidaan tarvittaessa hallita mobiililaitteina, joille sovelluksia tarjotaan Windows-kaupan kautta.

Windows Intunen hallinnan avulla mobiililaitteet saadaan samaan näkymään muiden päätelaitteiden kanssa. Tällöin pystytään paremmin valvomaan, mitä laitteita käyttäjät käyttävät ja määrittelemään, mitä laitteilla saa tehdä, ja jakamaan yrityksen käyttämiä sovelluksia niin valmistajien virallisista kaupoista kuin myös suoraan. Yritysportaaliin voidaan jakaa myös linkkejä muihin internetsivustoihin.

MDM:n avulla päästään laitteita hallitsemaan suoraan laitteen rajapinnan, API:n avulla. Etätoimenpiteisiin, käyttöjärjestelmästä riippuen, kuuluu mahdollisuus laitteen etätyhjennykseen, etälukitukseen sekä turvakoodin palauttamiseen. Muut hal-

linnan määritykset tehdään käytäntösääntöjen avulla. Intunen puolella käytäntösääntöjä on pitkä lista, mutta koska laiteperheitä on useita ja käytetyt API-rajapinnat ovat erilaisia, kaikki säännöt eivät kosketa jokaista mallia.

Office 365:den puolella mobiililaitteiden hallintaan on käytössä EAS, Exchange ActiveSync, joka sisältää jo vakiintuneita käytäntöjä puhelinten hallintaan. EAS:n avulla määritellään turvallisuussääntöjä, jotka palveluun kytkeytyvän laitteen on täytettävä. Office 365:den EAS-hallinnan piirissä olevat mobiililaitteet on mahdollista tuoda mukaan Intunen piiriin erillisellä Service to Service Connectorilla, joka synkronoi laitteiden tiedot Exchangesta Intuneen. MDM:n käytön ei tarvitse korvata EAS:n käyttöä, vaan MDM-hallintaa voidaan ajatella EAS:n ominaisuuksien laajentamista laitekohtaisilla ominaisuuksilla.

4.3.2 ASENNETTUJEN OHJELMISTOJEN HALLINTA

Seuraava vaatimus kosketti tietoa asennetuista ohjelmistoista ja lisensseistä. Nämä molemmat ominaisuudet ovat olleet mukana Intunen alkuversioista lähtien, joten näihin ei ole tarvetta syvällisemmin perehtyä.

Kohdeyrityksessä olisi kuitenkin syytä automatisoida käyttöoikeuksien seurantaa, ja tämä onnistuisi hyödyntämällä Intunen käyttöoikeussopimuksien kirjaamista. Tämän jälkeen käyttöoikeussopimuksen raportit saadaan suoraan raporttinäkymästä. Lisäksi sopimuksia voi kohdistaa ryhmäkohtaisesti, jolloin käyttäjämäärien seuraaminen on helppoa.

4.3.3 ETÄTOIMENPITEET TIETOKONEILLE

Kolmas vaatimusryhmä koski laitteille mahdollistettavia etätoimenpiteitä. Mobiililaitteiden osalta tämän osion asioita käsiteltiin jo MDM-hallinnan osiossa, joten rajoitan tämän vaatimuksen koskemaan tietokoneita.

Tietokoneille suoritettaviin etätoimenpiteisiin kuuluvat muun muassa käskyt suorittaa haittaohjelmien tarkastuksia, käynnistää tietokone uudelleen, päivittää haittaohjelmatunnisteita ja käytäntöjä sekä resurssiluettelon päivittäminen. Lisäksi kone

voidaan poistaa Intunen hallinnasta, jolloin Client-ohjelmisto poistuu tietokoneelta, mutta muuten tietokoneen ohjelmiin ja asetuksiin ei puututa.

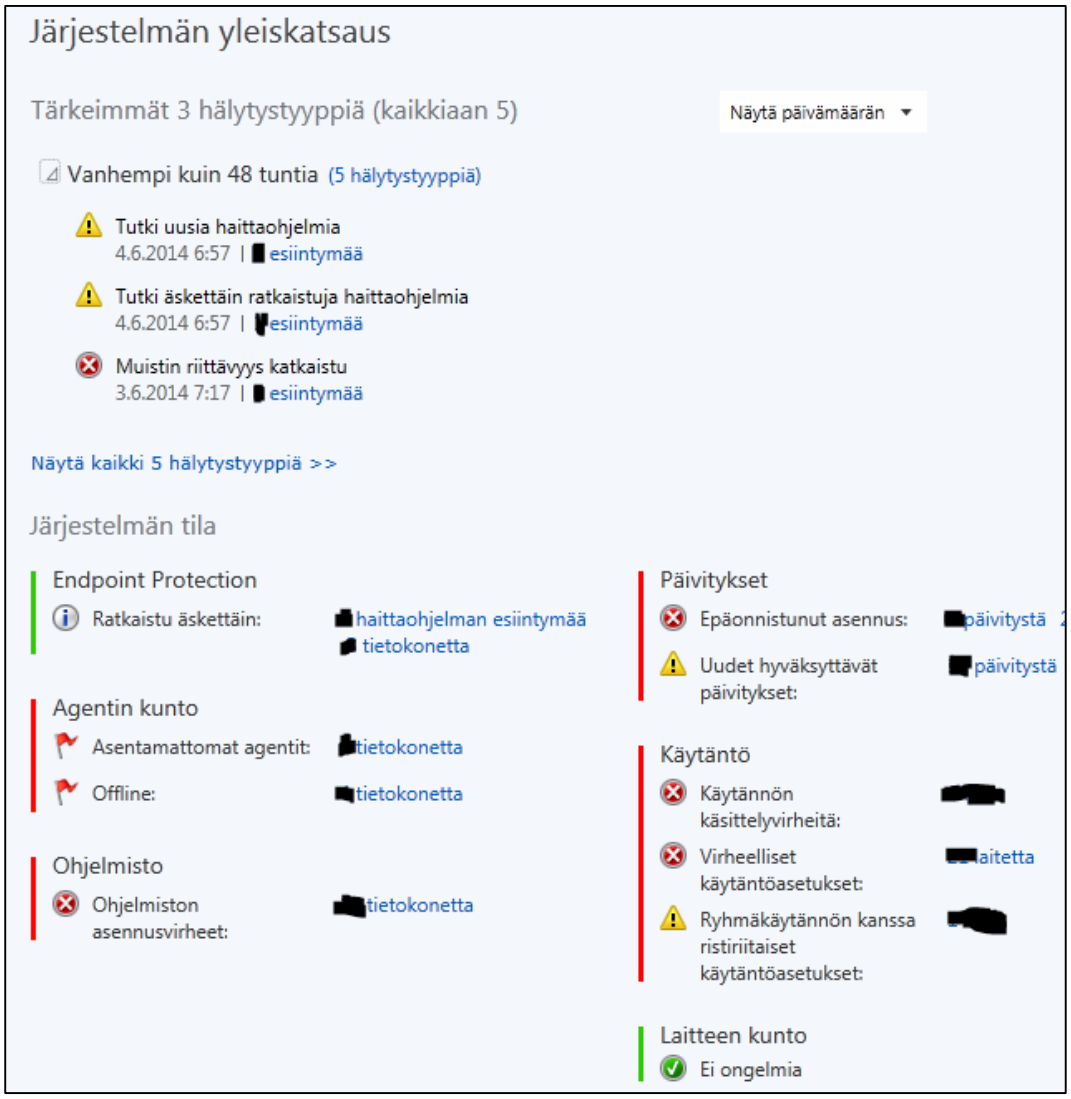
Koska tietokoneen poistaminen Intunen hallinnasta ei pyyhi laitteen tietoja, kuten on mahdollista tehdä mobiililaitteiden kanssa, tulee mahdollisiin laitevarkauspauksiin varautua ennalta käyttämällä esimerkiksi BitLocker-asemansalausta ja riittävän vahvoja salasanoja koneelle kirjautumiseen. Samoin tietokoneita hallitusti Intunen piiristä poistettaessa tulee varmistua siitä, että yrityksen ohjelmat poistetaan laitteelta ennen koneen poistoa Intunesta.

Etätuen osalta Intunen ominaisuudet ovat menneet huonompaan suuntaan Windows 8 -julkaisun jälkeen. Intunen etätukiominaisuus ei ole tällä hetkellä lainkaan käytettävissä Windows 8 - ja 8.1 -käyttöjärjestelmien kanssa, vaan Microsoft suosittelee käyttämään kolmannen osapuolen tukiohjelmistoja.

Ohjelmistojen levityksessä Windows Intune on ollut käytössä jo sen käyttöönoton alusta asti. Vuosien mittaan hallittavien ohjelmistojen määrä on kasvanut. Nykyisin yrityksessä pyritään kaikki tarvittavat ohjelmistot levittämään Intunen kautta, jolloin käyttäjä ei tarvitse asennuksia ja päivityksiä varten paikallisen järjestelmänvalvojan tunnuksia. Ohjelmistojen ja päivitysten levitys ei ole sinällään muuttunut paljonkaan vuosien saatossa, vaan edelleen eri ohjelmistot käyttäytyvät hieman eri tavalla, ja nämä joudutaan ensin levittämään testiryhmän sisällä ennen laajempaa levitystä. Suurimpana muutoksena ohjelmistojen jakeluun on mahdollisuus jakaa myös mobiilisovelluksia, jota käsiteltiin MDM-hallinnan osiossa.

4.3.4 TIETOTURVAN VALVONTA

Windows Intunen avulla saadaan nopea yleiskuva kaikista palveluun liitetyistä päätelaitteista (kuva 19). Heti aloitussivun näkymässä on nähtävissä tuoreimmat hälytystyypit ja järjestelmän tila. Kaikkien ilmoitusten perässä on linkki esiintymään, jolloin kyseessä olevaa kohdetta ei tarvitse etsiä muuta kautta.



Kuva 19. Kohdeyrityksen päätelaitteiden yleiskatsausnäkymä Windows Intunessa kertoo nopealla katsauksella tärkeimmät asiat hallinnan kannalta.

Intune jakaa hälytystyypit vakavuuden mukaan kolmeen kategoriaan: vakava, varoitus ja tiedotus. Järjestelmänvalvoja pääsee halutessaan erikseen määrittämään hälytysten tilan ja vakavuuden. Samoin päästään valitsemaan hälytysilmoitusten vastaanottajat ja ilmoitussäännöt.

Järjestelmän sisäisiä ilmoitussääntöjä ovat etätukipyynnöt, kaikki hälytykset, kriittiset hälytykset, tiedotushälytykset ja varoitushälytykset. Näitä sääntöjä yritys ei pääse itse muokkaamaan, vaan valittavaksi jää ainoastaan, halutaanko näistä lähtevän sähköposti-ilmoitusta vai ei. Sen sijaan yritys pääsee luomaan omia ilmoitussääntöjä hälytysluokan, vakavuusasteen ja kohderyhmän mukaisesti.

Tiedot järjestelmän yleiskatsaukseen tulevat Windows Intunen sisäänrakennetuista tietoturvaominaisuuksista. Näihin kuuluvat muun muassa Endpoint Protection eli keskitetty virus- ja haittaohjelmasuojaus, palomuurin määritykset sekä ohjelmistojen ajan tasalla pitäminen keskitettyjen päivitysten avulla.

Endpoint Protectionin ja palomuurin asetuksien määritykset tapahtuvat Windows Intunen käytäntöjen avulla. Käytännöt perustuvat malleihin, joista käytettävät arvot valitaan yrityksen sääntöjen mukaiseksi. Käytäntöihin on tullut paljon lisäominaisuuksia lukuisien päivitysten kautta. Uudet ominaisuudet eivät tule käyttöön oletuksena vaan ne täytyy erikseen käydä kytkemässä päälle. Tapauksissa, joissa järjestelmän pääkäyttäjä ei ole määrittänyt käytännölle arvoa, loppukäyttäjä tai jokin toinen ohjelma voi määrittää tarvittavan käytännön. Tämä voi aiheuttaa laitteiden toimintaan eroja, joten jokaisen käytännön vaikutukset tulisi miettiä ennakkoon ja määritellä käytäntö käyttäjäryhmien tarpeiden mukaisesti.

4.4 OFFICE 365 TESTIYMPÄRISTÖSSÄ

Office 365:den ominaisuuksia tarvitaan testiympäristön kautta saatujen kokemusten mukaan kohdissa: 4, 5, 6, 8, 12, 13, 15, 16 ja 17. Kyseisten vaatimusten toimet voidaan jakaa tiedostojen hallintaan ja säilytettävyyteen (kohdat 5, 6, 12, 13 ja 15), mobiililaitteiden hallintaan (kohdat 4 ja 8) sekä tietoturvaan ja saavutettavuuteen (kohdat 16 ja 17). Office 365:ttä koskevat vaatimukset on koostettu taulukkoon 8. Useat vaatimuksien kohdat ovat sellaisia, että ne voitaisiin esittää myös jonkin toisen yhteisen tekijän kautta.

Taulukko 9. Vaatimukset, joihin vastauksia etsittiin Office 365:den avulla.

Nro	Vaatimus	Yhteinen tekijä
5	Käyttäjän omien tiedostojen saavutettavuus eri päätelaitteilla	Tiedostoihin pääsy ja tiedon suojaaminen
6	Yrityksen tiedostojen saavutettavuus eri päätelaitteilla	
12	Yrityksen tiedon suojaaminen	
13	Projektien tiedostojen hallinta	
15	Turvallinen sähköpostiliikenne	
4	Mobiililaitteiden hallinta	Mobiililaitteiden hallinta
8	Etätoimet laitteille	
16	Kadonneen salasanan hyödyntämisen havaitseminen	Tietoturva ja palveluiden saavutettavuus
17	Yhteysongelmatilanteisiin varautuminen	
1	*Kaikkien yritysten tietokoneiden hallinta riippumatta sijainnista*	
2	*Tiedot asennetuista ohjelmistoista ja niiden versioista*	
3	*Lisenssien hallinta järjestelmän avulla*	
7	*Tietoturvan valvonta ja määritykset*	
9	*Tiedon suojaaminen koneen kovalevyllä*	
10	*Käyttäjätuki etäyhteyden avulla*	
11	*Ohjelmistojen asennukset ja päivitykset*	
14	*Yhdet kirjautumistunnukset*	

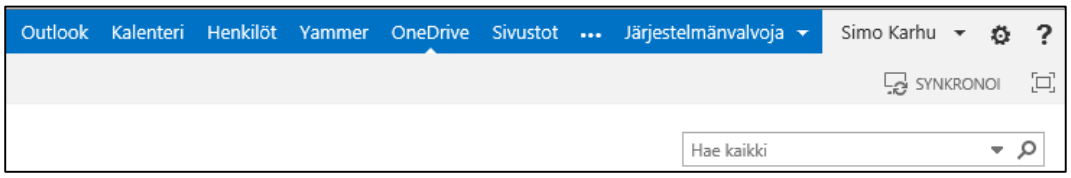
Kohdan 14 vaatimus SSO-kirjautumistunnuksista vaatii Active Directory -synkronoinnin DirSync-ohjelmiston avulla. Jos halutaan pysyä kokonaan pilvipohjaisessa infrastruktuurissa, voidaan AD:kin asentaa Azureen virtuaalikoneeksi. Näin omaa konesalia ei tarvita lainkaan. Tätä kohdan 14 vaatimusta ei kuitenkaan lähdetty tässä työssä toteuttamaan, koska vaade ei suoranaisesti liittynyt käsiteltyihin pilvipalveluihin.

4.4.1 TIEDOSTOJEN KÄYTTÖ

Office 365:den osalta yhdistin yrityksen tekemistä vaatimuksista käyttäjän omien ja yrityksen tiedostojen saavutettavuuden eri päätelaitteilla, yrityksen tiedon suojaamisen sekä projektien tiedostojen hallinnan yhdeksi vaatimukseksi: tiedostoihin pääsy ja tiedon suojaaminen.

SharePoint ja OneDrive for Business toimivat samalla SharePointin alustalla, joten näitä voidaan tässä työssä myös käsitellä yhtenä osiona. OneDrive on Microsoftin tunnuksilla tuleva yksityinen tallennustila, kun taas OneDrive for Business on yrityksen hallussa oleva käyttäjän henkilökohtainen työtiedostotila. SharePointin työtilat ovat puolestaan useimmiten projekti- ja työryhmäkohtaisia jaettuja tiloja. Jos käyttäjä haluaa jakaa jonkin tiedoston koko organisaation käyttöön, hän voi laittaa sen OneDrive-asiakirjatilan ”jaettu kaikille” -kansioon. Tämän jälkeen tiedosto on löydettävissä SharePointin haun kautta. Yksittäisen asiakirjan tai kansion käyttäjä voi jakaa järjestelmänvalvojan määritysten mukaisesti joko vain yrityksen sisällä tai myös yrityksen ulkopuolelle.

OneDrive for Business toimii nykyisin jo lähes kaikilla alustoilla suoraan sovelluksesta käsin, joten käyttäjän tiedostojen käsittely eri laitteilla on helppoa. Käytettäessä muuta kuin omaa päätelaitetta, palveluun mennään samaa tietä kuin kaikkiin muihinkin Office 365:den palveluihin: selaimen avulla osoitteesta ”https://portal.microsoftonline.com”, tai ”https://portal.office.com”. Sivustolle kirjautumisen jälkeen yläpalkin siirtymistoiminnot ovat kuvan 20 mukaiset.

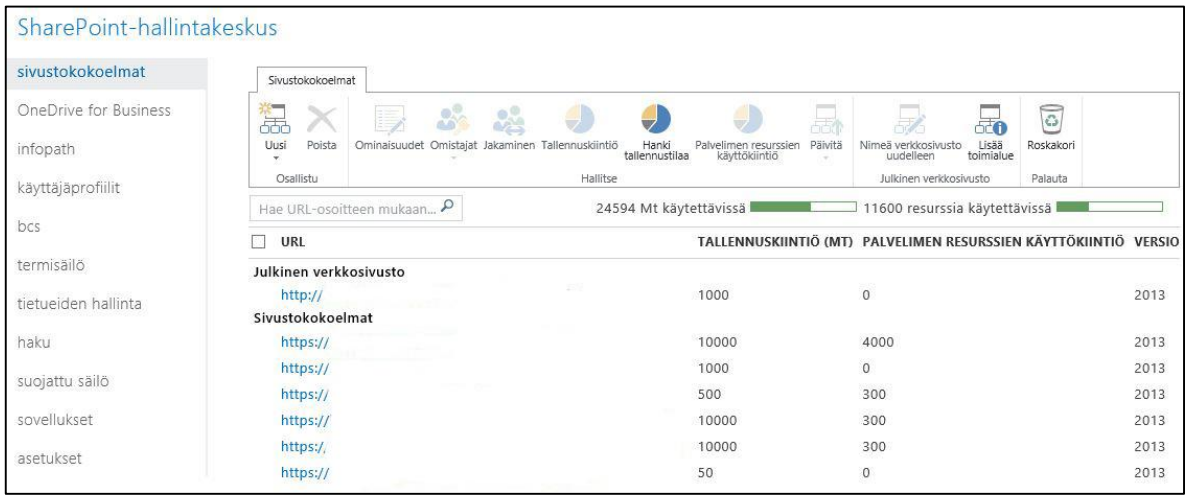


Kuva 20. Ruutukaappaus Office 365 sivuston siirtymisnäkymästä.

Tämän osoitteen kautta käyttäjä pääsee käsiksi tiedostoihinsa kaikilta päätelaitteilta. Laitteessa ei tarvitse olla asennettu Office-ohjelmistoja, vaan tiedostoja voidaan käyttää perusmuokkaukseen Online-ohjelmilla tai suurempia rakenteellisia muutoksia varten Office on Demand -palvelun kautta. Tiedostot aukeavat oletuksena Online-ohjelmistoihin, mikä on siirtokaistan kulutuksen takia nopein muokkausvaihtoehto. Tiedostot sijaitsevat pilvipalvelimella, joten myös muokkaus tuolla samalla palvelimella on nopeampaa kuin ladata tiedosto käyttäjän koneelle muokattavaksi.

OneDrive for Business -sovellus asentuu käyttäjän koneelle uusimman Office 2013 -asennuksen yhteydessä, ja tämän jälkeen käyttäjän haluamat tiedostot näkyvät resurssienhallinnan kautta myös yhteydettömässä tilassa. Jos tiedostoihin tehdään muutoksia, ne päivittyvät palvelimelle, kun verkkoyhteys on taas käytettävissä. Koska OneDrive for Business ja SharePoint käyttävät samaa alustaa, voidaan myös halutut SharePoint-kirjastot synkronoida käyttäjän tietokoneelle. Resurssienhallintanäkymä voi helpottaa käyttäjien siirtymistä perinteisistä jaetuista asemista SharePointin kirjastojen käyttöön.

SharePointin työryhmä- ja projektitiloja voi tehdä sivustolle pk-yrityksen tarpeisiin vähintäänkin riittävästi. Tiloja luodessa on kuitenkin syytä miettiä, onko kyseiseen alueeseen tarvetta päästä organisaation ulkopuolelta ja vaarantaako tämä mahdollisesti yrityksen tietoturvan. Tällaisille projekteille onkin syytä luoda kokonaan oma sivustoryhmä, jolloin muut dokumentit saadaan varmasti eroteltua projektikohtaisista dokumenteista ja ulkopuoliselta pääsyltä. Sivustoryhmien luominen tapahtuu SharePointin hallintakeskuksesta (kuva 21), jonka kautta voidaan luoda tilauksesta riippuen 1-10 000 sivustokokoelmaa, joissa kussakin kokoelmassa voi olla 2000 sivustoa [59].



Kuva 21. SharePoint-hallintakeskuksen sivustokokoelmat ja resurssien käyttökiintiöt

Yrityksen tiedon suojaamiseksi palveluissa on useita mahdollisuuksia, joista tiedon jakaminen eri sivustokokoelmille on vain yksi. Pilvipalveluissa on erityisen tärkeää

määritellä, kuinka palveluissa oleva tieto saadaan pidettyä vain sitä tarvitsevien hallussa. Tätä tarkoitusta varten Office 365:den E3 -palvelupaketin ominaisuudet ovat huomattavasti laajempia kuin pienemmille yrityksille suunnatut tuotteet.

Käyttöoikeuksien hallinta on tietojärjestelmien perusominaisuus, mikä liittyy kaikkiin yrityksen järjestelmiin. Myös Office 365 -tiliä luotaessa määritetään, mihin sovelluksiin käyttäjällä on oikeudet. Tämä määrittää perustason pääsyoikeudet ohjelmistoihin, joiden sisällä voidaan käyttöoikeudet määritellä aina tiedostotasolle asti. Perinteisten käyttöoikeusmääritysten lisäksi Office 365 tuo uusia kehittyneitä ratkaisuja tiedon suojaamiseen.

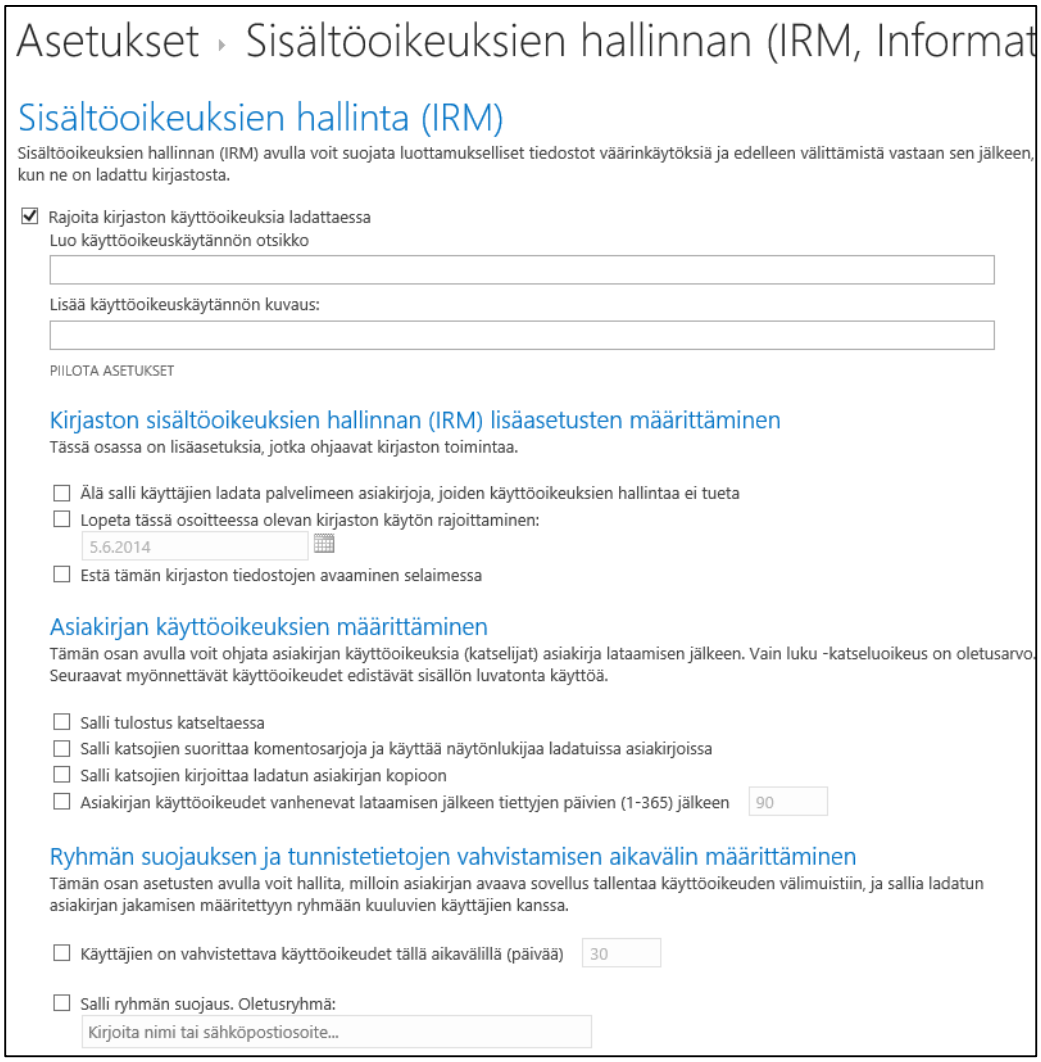
4.4.2 SISÄLTÖOIKEUKSIEN HALLINTA

Yrityksen luottamuksellisen tiedon säilyttämiseksi tulee Office 365:den hallintakeskuksesta kytkeä päälle oikeuksien hallinta. Sisältöoikeuksien hallinta, IRM (Information Rights Management), on Office 365:den E3-tasoon sisältyvä ominaisuus, jolla pystytään monipuolisesti suojaamaan yrityksen tietoja. Sisältöoikeuksien hallinta käyttää Windows Azure Active Directory Rights Management (Azure RMS) –palvelua, ja sisällönhallintaa voidaan hyödyntää Office-ohjelmistoissa, SharePointissa ja sähköpostissa. IRM:n avulla pystytään suojaamaan yrityksen tärkeät dokumentit muun muassa siten, ettei niitä voida tulostaa, lähettää eteenpäin, ladata tai kopioida.

Sisältöoikeuksien hallinta tulee kytkeä erikseen päälle Office 365 -hallintapaneelista haluttuihin palveluihin. Oletuksena palvelun kytkemisen jälkeen Office-ohjelmistoihin tulee tiedon suojaamiseksi käyttöön kaksi valmista suojausmenetelmää: salainen ja salainen pelkillä lukuoikeuksilla. Tiedon määrittäminen salainen-mallin mukaiseksi tarkoittaa sitä, että tieto on tarkoitettu vain yrityksen sisäiseen käyttöön. Tiedostoa ei voi kopioida tai tulostaa. Tiedon jakamisen pystyy määrittämään myös pelkästään joillekin henkilöille tai ryhmille halutuin käyttöoikeustasoin. Haluttuja valmiita tiedon suojaamisen malleja pystytään luomaan lisää Azuren RMS-palvelun kautta. Azuren kautta pystytään määrittämään tiedon käsittelysääntöjen

lisäksi muun muassa sisällön vanhenemisesta ja tiedon saatavuudesta yhteydettömässä tilassa.

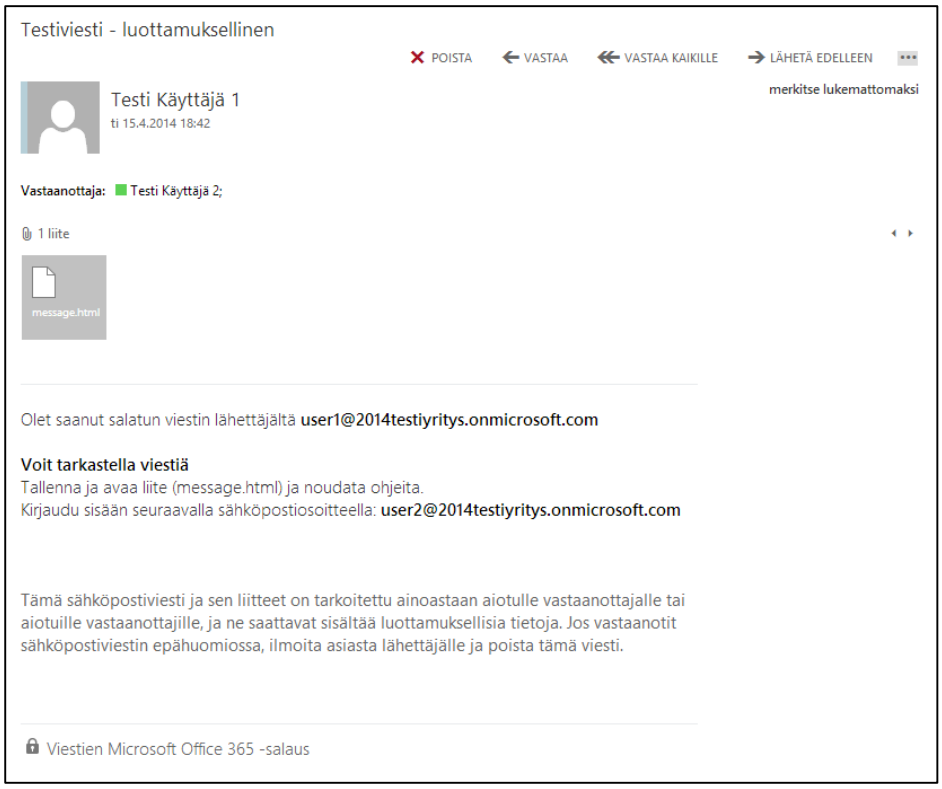
SharePointissa sisältöoikeuksien hallinta kytketään sivustokokoelmatasolla päälle tai pois, oletuksena palvelu ei ole päällä. IRM:n käyttöönoton jälkeen sisältöoikeuksia voidaan hallita kirjastokohtaisesti. Sisältöoikeuksilla voidaankin täydentää käyttöoikeuksilla määritetyn kirjaston sisältämien tiedostojen käyttötarkoitusta. Perinteisesti tiedostojako on määritetty henkilö- tai ryhmäkohtaisesti, mutta tiedostot ovat suojattuja vain tuossa sijainnissa. Jos tiedosto on kopioitu toiseen kansioon, myös tiedostoon pääsy vaihtuu. Sisältöoikeuksien hallinnalla voidaan estää tiedostojen joutuminen yrityksen ulkopuolisiin sijainteihin (kuva 22). Sisältöoikeuksilla määritetyt oikeudet säilyvät tiedostolla, vaikka sen kopiointi toiseen sijaintiin olisikin sallittu, salattu tiedosto pysyy edelleen salattuna ja esimerkiksi tulostamisen esto toimii sijainnista riippumatta myös yhteydettömässä tilassa. Asiakirjat saadaan myös tarvittaessa vanhenemaan halutun ajan kuluttua, jolloin niiden käyttö estyy.



Kuva 22. SharePoint-kirjastojen suojaaminen sisältöoikeuksien hallinnan avulla tuo useita suojausmekanismeja tiedostotasolle asti.

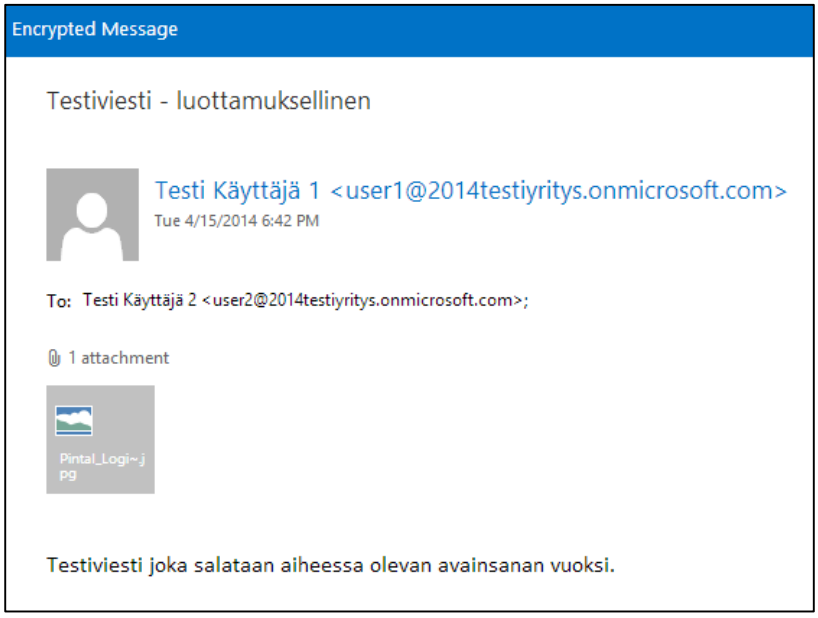
Sähköpostisovellukseen IRM tuo viestin käyttöoikeusvalinnan taakse automaattisesti palvelun päälle kytkennän jälkeen kohdat: älä lähetä edelleen, salainen ja salainen - vain luku. Lisäksi Exchange-ylläpitokeskuksen kautta voidaan luoda uusia sääntöjä, mitä tietoa yrityksestä voidaan lähettää. Viestin sisältä voidaan esimerkiksi tunnistaa luottokorttinumeroita sekä henkilötietoja sisältävät viestit ja varoittaa käyttäjää tai kokonaan estää näiden tietojen lähettäminen yrityksen ulkopuolelle. Uusimpana ominaisuutena Office 365:een on tullut sähköpostiviestien automaattinen salaaminen luotujen sääntöjen perusteella.

Testiympäristössä loin säännön, jolla kaikki lähtevät viestit salataan käyttäen Office 365 –salausta, jos viestin aiheessa on teksti luottamuksellinen, salassa pidettävä tai salaus. Itse säännön saa luotua melko vaivattomasti Exchange-ylläpitokeskuksen sääntöjen kautta, mutta ongelmaksi muodostui alkuun virheilmoitus IRM-lisensoinnin puuttumisesta. IRM-lisensoinnin käyttöönotto täytyi tehdä Windows Azure Active Directory Module for Windows PowerShell -työkalun avulla. PowerShellillä täytyi määrittää RMS Online -salausavaimen sijaintipaikka ja Trusted Publishing Domain (TPD) eli luotettu julkaisupaikka sekä lopuksi ottaa IRM-lisensointi käyttöön. Näiden toimien jälkeen viestien salaus saatiin toimimaan aiotulla tavalla, ja salatun viestin lähettäminen tapahtuu samoin kuin normaalin sähköpostiviestin lähetys; salauksen ottaminen viestissä käyttöön perustuu vain ennalta määrättyihin sääntöihin. Kuvan 23 tapauksessa käytettiin aihekentässä ennalta määritetyn säännön mukaisesti sanaa luottamuksellinen, ja tämä sai aikaan viestin salauksen ilman muita käyttäjän toimia. Viestin salauksen käyttöönottamiseksi löytyy säännöistä monia eri asetuksia, joilla saadaan aikaan haluttu käytäntö.



Kuva 23. Salatun viestin saapumisen ilmoitus Outlook OWA -ohjelmassa.

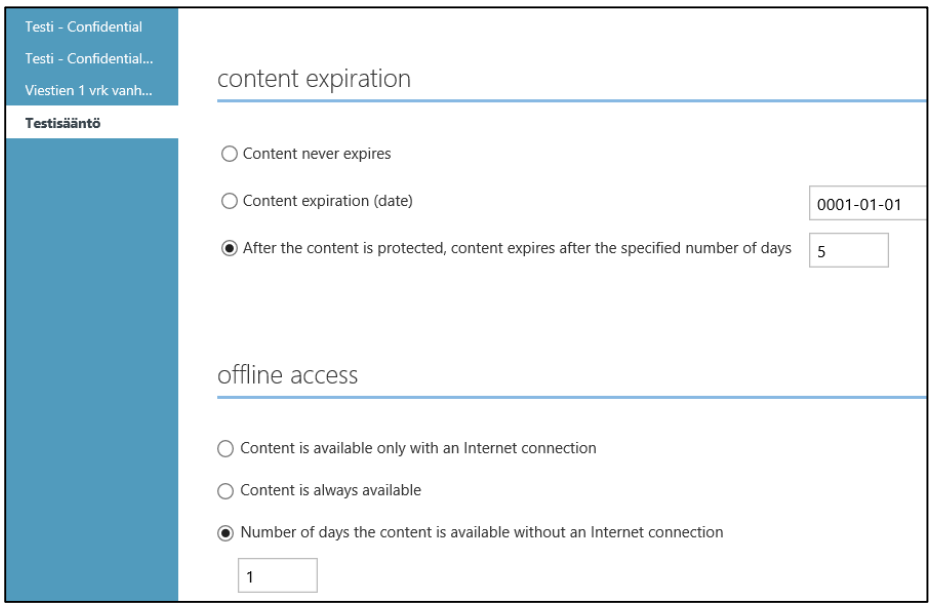
Salattu viesti sisältää message.html-tiedoston, joka tulee ladata ja avata. Käyttäjän identifiointi tapahtuu joko Microsoft-tilin (hotmail.com, live.com, outlook.com) tai organisaatiotilin (Office 365) kautta. Jos vastaanottajan sähköpostitiliä ei ole yhdistetty Microsoftin tiliin, pyytää palvelu ensimmäisellä käyttökerralla luomaan tunnukset viestin lukemista varten. Salatun viestin ilmoituksen tekstit ja otsikot, sekä halutessaan myös yrityksen logon saa muokattua haluamakseen PowerShellin avulla. Näillä viestin personointitavoilla voidaan kasvattaa luottamusta viestin sisältöön, jos vastaanottaja ei osaa odottaa salattua viestiä kyseiseltä lähettäjältä. Kuvassa 24 näkyy alkuperäinen lähetetty viesti, jossa liitteenä lähetettiin kuvatiedosto.



Kuva 24. Salattu viesti avattuna viestin lukutilassa. Viestin salaaminen perustui sääntöön, joka etsi aihekentästä sanan luottamuksellinen.

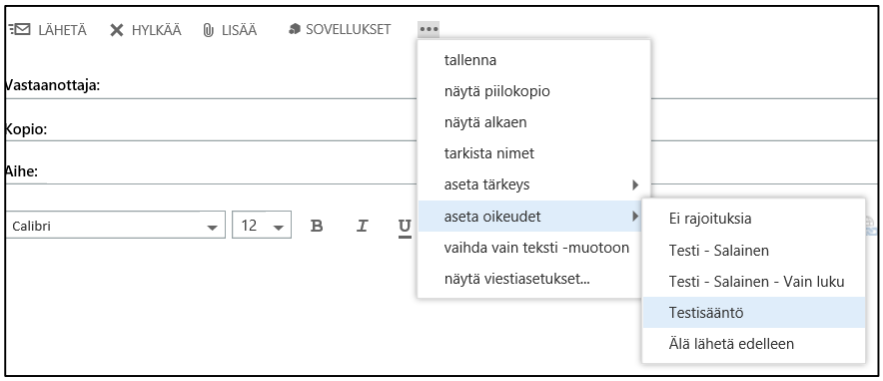
Salattuun viestiin vastaaminen tai viestin edelleen välittäminen salaa oletusasetuksilla myös tämän viestin automaattisesti, vaikka otsikkokentästä poistettaisiin salauksen alun perin aiheuttanut sääntö. Tällä varmistetaan koko viestiketjun pysyminen salattuna. Lisäksi salattu viesti ei näy selkokielisenä käyttäjän postilaatikossa, vaan vaatii aina kirjautumisen lukutilaan. Säännöillä on mahdollista luoda myös käytäntö, joka poistaa vastauksista salauksen esimerkiksi, jos viestin saajan osoite sijaitsee organisaation sisällä.

Jos viestien salaamista ei haluta käyttää, mutta halutaan estää viestien jääminen vastaanottajan postilaatikon uumeniin, niin tehokas keino suojata sähköpostiviestien tiedostot on käyttää Azuren Rights Management -palvelun sääntöjä suojattujen kohteiden vanhenemiselle. Tämän toiminnan todentamiseksi luotiin Azuren RMS-hallintanäkymästä sääntö viestien vanhenemiseksi viidessä vuorokaudessa ja yhteydettömän tilan säilytykseksi enintään yhden vuorokauden (kuva 25). Tämän jälkeen jaettu tiedosto ei ole enää käytettävissä, vaikka se olisi ladattu talteen.



Kuva 25. Azuren RMS:n avulla luotu testisääntö sisällön vanhenemisesta ja käytettävyydestä tulee luonnin jälkeen käytettäväksi muihin Officen ohjelmiin.

Azuren kautta luotu testisääntö on luomisen jälkeen käytettävissä Officen ohjelmissa. Tämä löytyy samoista valikoista kuin salaiseksi määrittelemisen tiedot (kuva 26). Säännöt kannattaakin tehdä selkeillä nimillä, jotta loppukäyttäjän olisi helppo valita tarvittava sääntö käyttöön.



Kuva 26. Azuren RMS avulla luodut säännöt saadaan tarvittaessa kaikkien organisaation käyttäjien käytettäväksi suoraan valikkojen kautta. Kuvassa aiemmin luotu testisääntö on näkyvissä oletusoikeuksien seassa.

Myös Outlook Web Appin, josta yleisesti käytetään lyhennettä OWA, käyttöä varten Exchange-ylläpitokeskuksesta voidaan luoda omat käytännöt eri käyttäjäryhmille. OWA-ohjelmistoa käytetään, kun sähköpostiin kirjaudutaan Internet-selaimen kautta mutta myös joissakin mobiililaitteissa. Koska Internetin kautta sähköpostia käytettäessä usein käytössä on jokin yleinen tietokone, tulee myös tiedostojen käyttöön kiinnittää huomiota. Outlook Web Appin käytäntöjen avulla voidaan määrittää muun muassa, mitä osioita postilaatikkosovelluksesta pystytään käyttämään, miten tiedostot avautuvat tai voidaanko liitteitä ylipäätänsä tarkastella muualla kuin selaimessa ja voidaanko sähköpostia käyttää myös offline-tilassa.

4.4.3 MONIVAIHEINEN TODENTAMISMENETTELY

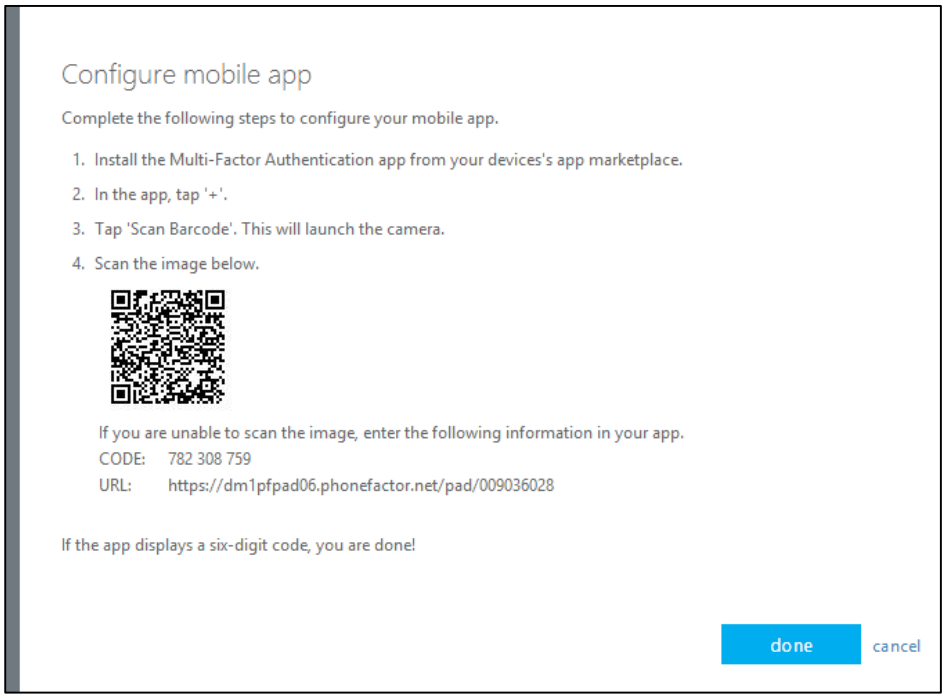
Koska pilvipalvelut ovat käytettävissä miltä tahansa laitteelta selaimen avulla, tulee käyttäjän todennukseen kiinnittää erityistä huomiota. Jos käyttäjän tunnus- ja salasanayhdistelmä ovat tiedossa, voi kuka tahansa kirjautua näillä tunnuksilla käyttäjän tilille myös muualta kuin yrityksen tiloista käsin.

Ensimmäisenä asiana käyttäjätilin suojaamisessa on salasanakäytännöt. Salasanan tulee olla riittävän monimutkainen ja pitkä, jotta se ei ole arvattavissa. Lisäksi salasanan vanhenemiskäytännöt tulee määrittää järkevälle tasolle. Käyttäjillä on kuitenkin taipumus kirjoittaa salasanojaan näkyville, joten näissä tapauksissa edellä

mainituilla toimilla ei ole vaikutusta. Tällaisissa tapauksissa voidaan harkita henkilö- tai ryhmäkohtaisesti Online-ohjelmistojen käytön rajoittamista käytäntösääntöjen avulla joko kaikilla tietokoneilla tai vain julkisilta koneilta käytettäessä.

Käytäntösäännöillä toimintoja voidaan rajoittaa sovelluskohtaisesti riippuen siitä, käytetäänkö palveluita yksityiseltä tai julkiselta koneelta. Palveluiden käytön kokonaan estäminen on myöskin mahdollista, mutta sotii mielestäni pilvipalveluiden ajatusmallia vastaan. Esimerkiksi Outlook Web App (OWA) ohjelmiston käyttö on uusimmissa versioissa niin ominaisuuksiltaan kuin ulkoasultaan hyvin lähellä Outlookin työpöytäversiota. OWAn käyttö onkin nykyisin jo niin sujuvaa, että työpöytäohjelmiston käytölle ei ole juurikaan erillistä tarvetta. Tämän vuoksi monet käyttävät OWA-ohjelmistoa myös työkoneillaan, joten ominaisuuksien pois rajoittaminen tulisi rajoittamaan myös työskentelyn tehokkuutta. Parempi vaihtoehto palveluiden kieltämiselle on varmistua käyttäjän henkilöllisyydestä, ja tähän tarkoitukseen Office 365:dessä on nykyisin MFA, Multi-Factor Authentication, joka tässä tapauksessa toimii kaksivaiheisena todentamisena.

Testiympäristössä otin osalle käyttäjistä käyttöön MFA-todentamisen. Kokeilin käyttäjän lisätodentamisena niin tekstiviestillä saatavaa kuusinumeroista koodia kuin myös mobiilisovelluksen kautta tapahtuvaa todentamista. Molemmat vaihtoehdot toimivat kuten piti, ja varsinkin mobiilisovelluksella käyttökokemus oli erittäin sujuva, koska erillistä numeroiden syöttämistä ei tarvittu. Kuvassa 27 on esitetty mobiilisovelluksen käyttöönotto 2D-viivakoodin avulla. Sovelluksille, jotka eivät toimi internetselaimen kautta, tulee kaksivaiheisen todentamisen käyttöönotossa luoda erillinen sovellussalasana. Office-blogin mukaan myös perinteisten työpöytäsovellusten osalta monivaiheiseen todentamiseen on tulossa muutoksia vuoden 2014 aikana, ja erillinen sovellussalasana on vain välivaihe kohti muita todentamistekniikoita [60].

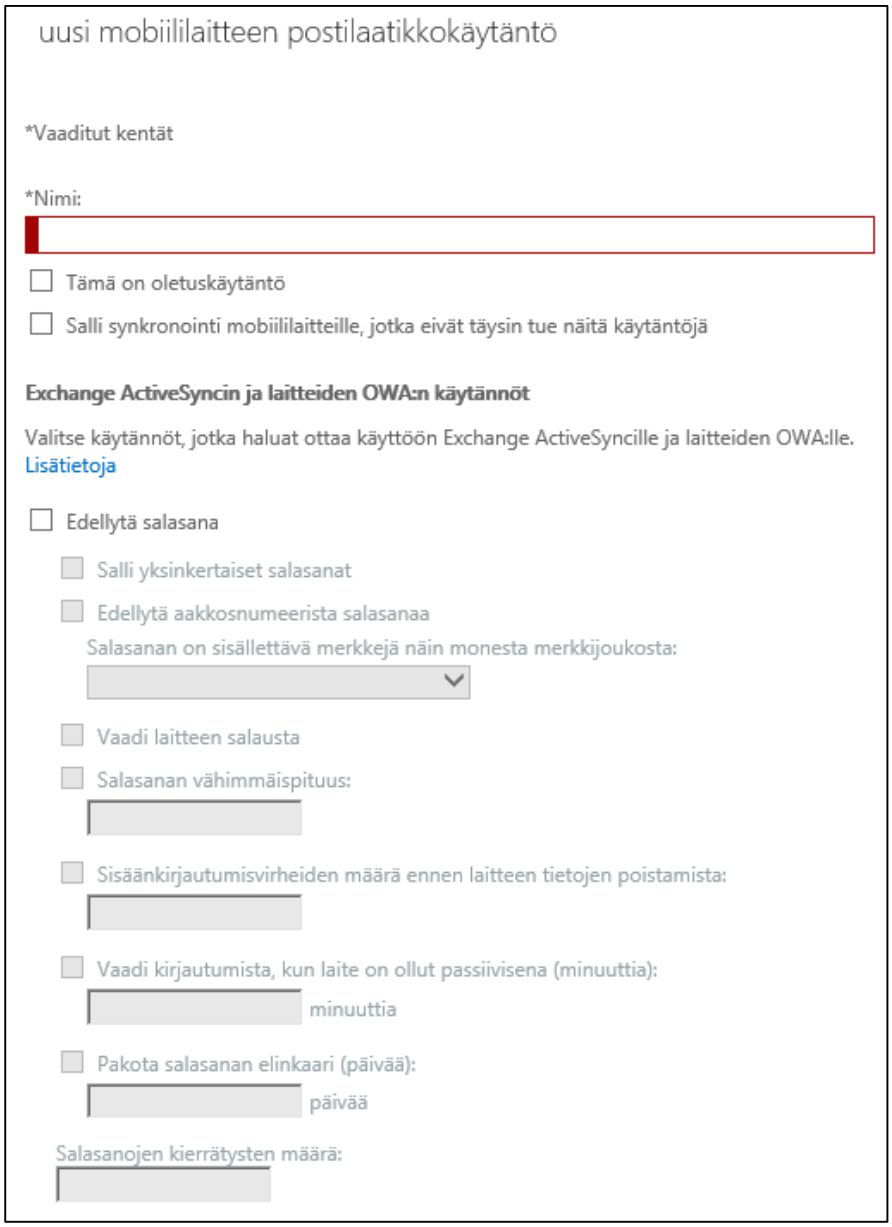


Kuva 27. Monivaiheisen tunnistautumisen mobiilisovelluksen käyttöönotto tapahtuu helpoimmillaan 2D-viivakoodin avulla.

4.4.4 MOBIILILAITTEIDEN HALLINTA

Kuten Windows Intunea käsittelevien kappaleiden kohdalla todettiin, myös Office 365:den avulla voidaan hallita mobiililaitteiden suojauskäytäntöjä. Hallinta hoidetaan Exchange ActiveSync (EAS) -protokollan avulla. EAS-protokolla on työkalu, jolla mobiililaitteet yhdistetään organisaation tietoihin Microsoft Exchange -palvelimella.

EAS:n sisältämien turvallisuusominaisuuksien avulla voidaan pakottaa puhelimen suojauskoodi päälle tilanteissa, joissa puhelimeen on liitetty yrityksen sähköpostitili. Näin puhelimiin saadaan asetettua halutun tasoinen suojaus (kuva 28), joka kytkeytyy säädetyn käyttämättömyysajan jälkeen päälle. Puhelimen suojakoodi estää pääsyn mobiililaitteen ja täten myös yrityksen järjestelmän tietoihin. Lisäksi katoamistapauksissa Exchange Onlinen avulla voidaan puhelin palauttaa täysin alkuperäiseen tilaan tiedot pyyhittynä.



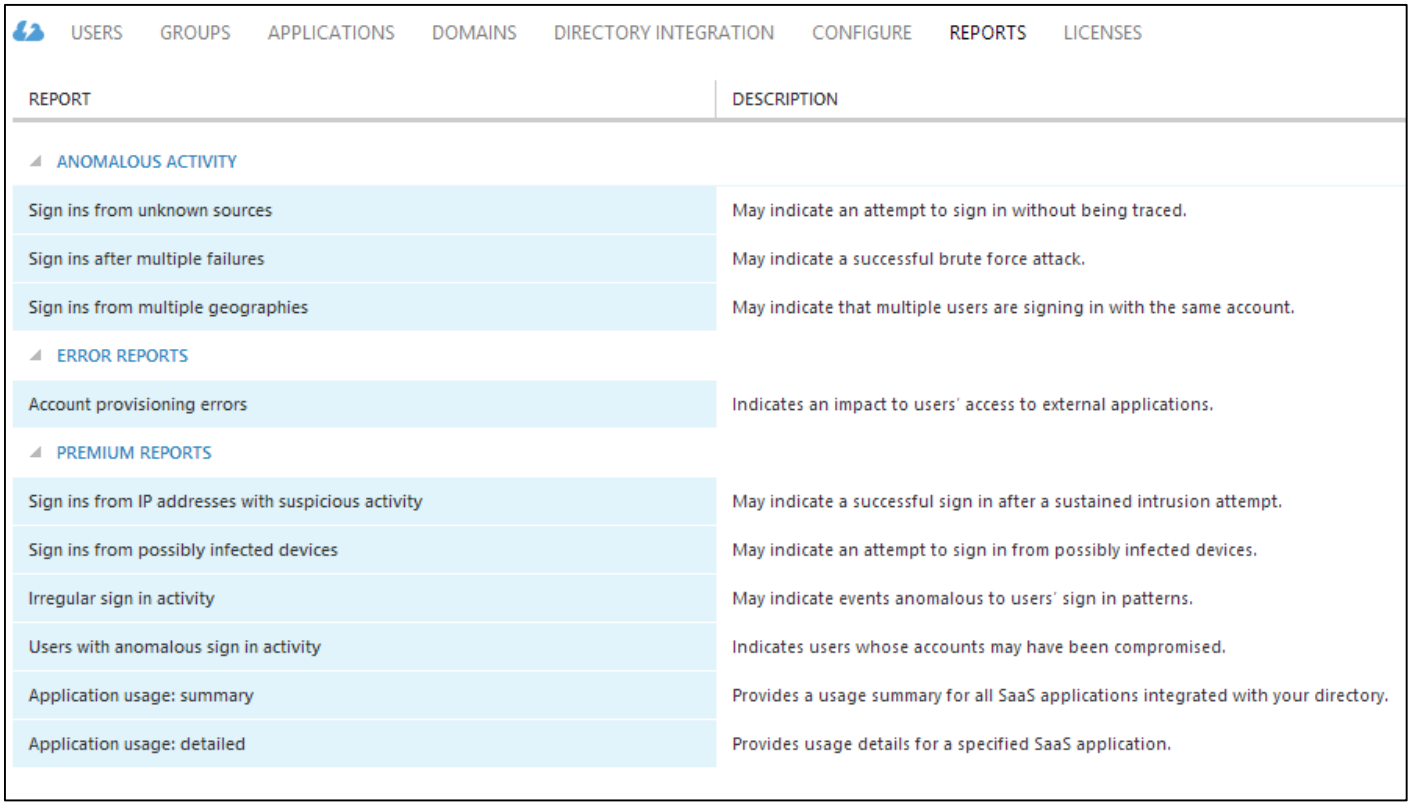
Kuva 28. Exchange ActiveSyncin avulla määritettävät mobiililaitteiden postilaatikkokäytännöt

Postilaatikkokäytäntöjä voi olla yrityksellä useita eri käyttäjäryhmiä varten. Käytäntöjen lisäksi matkapuhelimet voidaan laittaa automaattisesti karanteeniin, josta pääkäyttäjä voi valita, sallitaanko kyseisen mobiililaitteen käyttää yrityksen järjestelmiä.

4.4.5 TIETOTOTURVA JA YHTEYSONGELMIIN VARAUTUMINEN

Yksi yrityksen tekemistä vaatimuksista koski salasanan väärinkäytöksen havaitsemista. Käyttäjätunnusten väärinkäyttö on oleellinen riski pilvipalvelujen tapauksessa. Väärinkäyttöä pystytään vaikeuttamaan huomattavasti ottamalla käyttöön edellä esitelty monivaiheinen todentaminen, mutta Office 365 yhdessä Azuren kanssa tarjoaa tähän myös muita vaihtoehtoja.

Windows Azure Active Directory -palvelun raporttien avulla saadaan käyttäjien kirjautumisista paljon lisätietoja, joiden avulla voidaan todeta mahdolliset ulkopuoliset kirjautumiset ja kirjautumisyritykset (kuva 29).



Kuva 29. Windows Azure Active Directoryn raporttien avulla voidaan havaita ulkopuoliset kirjautumisyritykset.

Yhteysongelmiin varautumista tulee pohtia kahdelta kannalta, internetyhteyksien ja palvelun toimivuuden näkökulmasta. Itse Office 365 palvelulle Microsoft lupaa 99,9 % saavutettavuuden. Itse pilvipalveluiden toimivuuteen asiakasyrityksellä ei ole mahdollisuutta vaikuttaa. Palveluiden toimivuuden osalta käyttäjän huoleksi jää

verkon toimivuuden takaaminen. Mutta koska Office 365 toimii pilvipalveluna ja on saavutettavissa lähes kaikkien päätelaitteiden avulla, yrityksen kiinteän verkon kriittinen merkitys pienenee. Käyttäjillä on pääsy sähköposteihin ja muihin yrityksen dokumentteihin jopa toimipisteen sähkökatkojen aikana matkapuhelimien kautta. Tämä vähentää yrityksen toiminnan haavoittuvuutta.

4.5 PILVIPALVELUIDEN KUSTANNUSTEN ARVIOINTI

Oman konesalin kustannuksia laskettaessa monesti huomioidaan vain kustannukset, jotka tulevat laitteiden, sovellusten ja lisenssien hankinnasta ja unohdetaan muut kustannukset. Samoin pilvipalveluiden osalta huomioidaan vain kuukausittainen maksu. Kuitenkin molemmissa toimintatavoissa syntyy paljon muitakin kustannuksia. Näitä ovat muun muassa:

- Sähkölaskut kun palvelimet ovat päällä ympärivuorokautisesti
- Tietoliikennekustannukset
- Mahdolliset tiedonsiirtokustannukset palvelimelta poispäin ennalta määritetyn datan siirtorajan jälkeen
- Talon sisäisten palvelinten noin viiden vuoden välein tapahtuva uusiminen
- Käyttökatkojen aiheuttamat kustannukset

[61]

Palveluiden sijaitessa yrityksen omissa tiloissa toimintaa ei rajoita ulkoinen verkko, vaan toiminta tapahtuu nopeassa sisäverkossa. Myös pilvipalveluiden siirtomekanismit tulevat jatkuvasti älykkäämmiksi ja vievät täten vähemmän kaistaa. Pilvipalveluiden ollessa kyseessä kaistaa tarvitaan tietojen siirtämiseen palveluun, mutta itse tietokannan haut ja sähköpostin lukeminen tapahtuvat suurelta osin palvelinpäässä ja tietokoneen offline-tiedostojen kautta. Tehokkaamman välimuistikäsittelyn ja tiedostojen verkkokäytöstä huolimatta pilvipalvelut tarvitsevat enemmän tiedonsiirtokaistaa kuin talon sisäiset palvelut. Tämä voi muodostua ongelmaksi suurissa toimistoissa, joissa on paljon palveluiden yhtäaikaisia käyttäjiä.

[61]

Pilvipalveluiden kustannuksien vertaaminen omassa konesalissa tuotettuihin palveluihin on vaikeaa. Molemmilla toimintatavoilla on omat hyötynsä, joiden vertaileminen kustannusten muodossa on hankalaa. Internetistä löytyy kuitenkin useita eri laskimia, joilla eri asioita voidaan ottaa huomioon laskettaessa kokonaiskustannusta usealle vuodelle. Yksi tällainen on http://www.softwareadvice.com/tco/ sivustolla oleva TCO (Total Cost of Ownership) -laskuri. Jokaista suurempaa käyttöönottoa tulisikin pohtia erikseen, mitä hyötyjä palveluilla saadaan ja millä kustannuksilla.

5 TYÖN TULOKSET

Tässä työssä tutkin Microsoftin pilvipalveluiden nykytilanteen ominaisuuksia kohdeyrityksen päätelaitteiden hallitsemiseksi sekä tiedonhallinnan tehostamisen mahdollisuuksia. Kohdeyrityksellä on ollut käytössä Microsoftin pilvipalveluratkaisuja jo vuosia. Käytön myötä esiin tulleiden tilanteiden ja yrityksen tarpeiden pohjalta tehtiin yrityksessä vaatimusmäärittely. Yrityksen esittämien vaateiden pohjalta työn tutkimusosio jaettiin loogisiin osakokonaisuuksiin. Kaikkiin yrityksen esittämiin vaateisiin ei tämän työn puitteissa voitu etsiä suoria vastauksia. Yrityksessä tehdyn vaatimusmäärittelyn esimerkkitilanteita käytettiin testiympäristön mallipohjana, jonka avulla pyrittiin löytämään vastaukset työn alussa esitettyihin tutkimuskysymyksiin.

Testiympäristön avulla päästiin testaamaan palveluiden tarjoamia mahdollisuuksia vaarantamatta yrityksen käytössä olevia järjestelmiä. Windows Intune ja Office 365 yhdistettynä Microsoft Azuren palveluilla tarjosi lukemattoman määrän uusia ominaisuuksia, joita yrityksessä ei ole vielä otettu käyttöön ja joita kaikkia ei voitu tässä työssä käsitellä. Tämän työn alussa tekemieni rajauksien mukaisesti päädyin keskittymään tietoturvallisuuden parantamisen mahdollistaviin ratkaisuihin, joista voisi olla hyötyä yrityksen toiminnalle.

Päätutkimuskysymyksenä oli:
Miten tutkittujen pilvipalveluiden uudet ominaisuudet voisivat parantaa kohdeyrityksen päätelaite- ja tiedonhallintaa?

Kohdeyrityksen ongelmana on ollut Windows Intunen ja Office 365:den toimiminen eri tunnuksilla. Office 365 toimii palveluntarjoajan kautta ja Windows Intune puolestaan suoraan Microsoftilta hankittuna versiona, eikä näitä palveluita ole saatu yhdistettyä Microsoftin nykyisillä työkaluilla. Tähän on kuitenkin palveluntarjoajan mukaan tulossa muutos pian, joten tulevaisuudessa palveluiden täysi hyöty saadaan kohdeyrityksen ulottuville ja työssäni käsittelin testiympäristössä tilannetta, jossa palvelut toimivat yhdessä samoilla tunnuksilla.

Windows Intunen julkaisun jälkeen palveluun on tullut lisää varsinkin Windows 8 - ja 8.1 -käyttöjärjestelmien myötä uusia ohjelmistojen julkaisumenetelmiä. Tietokoneiden hallinnan perusteet ovat kuitenkin säilyneet ennallaan, ja ohjelmistojen sekä päivitysten jakelut tapahtuvat jo nykyisin yrityksessä Windows Intunen avulla.

Päätelaitteiden hallinnan osalta suuret muutokset ovat kohdistuneet mobiililaitteisiin ja kohdistuvat niihin myös tulevaisuudessa. Mobiililaitteiden hallinta onnistui aiemmin lähes pelkästään Windows Intunen ja System Center Configuration Managerin yhteistyön avulla, ja tämä toteutus vaati yritykseltä omaa palvelinkapasiteettia. Uusimmissa päivityksissä Windows Intune on kuitenkin kehittynyt suuntaan, jossa mobiililaitteiden hallintaa voidaan tehdä täysin pilvipohjaisesti ja hallinnan mahdollistamat ominaisuudet kasvavat vielä tämän vuoden aikana tulevissa uusissa versioissa.

Kohdeyrityksen mobiililaitehallinta on toteutettu tällä hetkellä Office 365 Exchange Onlinen EAS -protokollan avulla. EAS:n avulla voidaan pakottaa mobiililaitteiden suojauskäytännöt tehokkaasti, mutta monipuolisempia laiteasetuksia ja ohjelmistojakeluja varten Office 365 tulisi yhdistää Windows Intuneen Exchange Connectorin avulla. Näin toimien kaikki yrityksen päätelaitteet ovat nähtävissä Intunen laitehallinnan kautta, ja laitteille voidaan tarpeen mukaan suorittaa etätoimia.

Myös tietokoneiden kohdalla päätelaitehallintaa voidaan tehostaa erityisesti ohjelmistojen lisenssien hallinnan osalta. Yrityksen omistamat ohjelmistolisenssit olisi mahdollista saada tehokkaampaan käyttöön hyödyntämällä Intunen käyttöoikeussopimuksien kirjaamista ja sisäänrakennettuja raportteja sekä käyttöoikeusryhmäkohtaista ohjelmistojen jakelua.

Kohdeyrityksen tiedonhallinnan tehostamiseksi tulisi yrityksessä ottaa tehokkaammin käyttöön Office 365:den mahdollistamat yhteistyötyökalut ja dokumenttienhallinnan ratkaisut. SharePoint Onlineen tulee rakentaa työryhmäkohtaiset työtilat, jonne yhteisiksi tarkoitetut tiedot sijoitetaan, ja OneDrive for Business tulee ottaa

käyttöön henkilökohtaisten työtiedostojen hallinnassa. Molemmilla ratkaisuilla tiedostoja voidaan käyttää verkkosivun lisäksi myös tietokoneen resurssienhallinnan kautta. Palveluiden kautta voidaan valita, mitkä tiedostot tulee olla käytettävissä myös verkottomassa tilassa.

Ensimmäinen tarkentava alakysymys tutkimuksessa oli:
Mitä mahdollisuuksia palvelut tuovat yrityksen kriittisen datan suojaamiseksi?

Tutkituilla pilvipalveluilla voidaan yrityksen tietoja suojata monella eri tavalla, ja NSA-vakoilutapauksen paljastumisen jälkeen suojausmenetelmät ovat tehostuneet huomattavasti useilla palveluntarjoajilla. Myös Microsoft on parantanut palveluidensa salausta kautta linjan ja ottanut useita muita tiedostojen suojauksen mahdollisuuksia käyttöön.

Microsoftin uusimpien päivitysten jälkeen käyttäjien tiedostot ovat kaikissa palveluissa salatussa muodossa niin siirron kuin myös levyllä olon aikana. Windows Intunen käyttö mahdollistaa myös käyttäjien tietokoneen tietojen salauksen BitLocker-salausmenetelmällä. BitLockerin käytön mahdollisuus sisältyy Windowsin Enterprise-käyttöjärjestelmiin, joiden käyttöoikeus sisältyy Windows Intunen täysversioon. Bitlockerilla suojatun tietokoneen tiedot ovat turvassa, vaikka tietokone varastettaisiin ja kiintolevy irrotettaisiin laitteesta.

Käyttäjien todentaminen on pilvipalveluiden tapauksessa erityisen tärkeässä roolissa. Käyttäjät pääsevät tietoihin käsiksi miltä tahansa päätelaitteelta, joten kriittistä tietoa käsittelevien henkilöiden osalta tulisi kytkeä päälle Office 365 -palveluun julkaistu monivaiheinen todentamismenetelmä, jolloin voidaan paremmin varmistautua kirjautujan olevan oikea henkilö.

Käyttäjien todentamisen jälkeen tiedot järjestelmissä on suojattu käyttäjäkohtaisten oikeuksien mukaisesti. Yrityksen kriittisen tiedon poisvuotaminen järjestelmän sisältä voidaan estää joko estämällä tiedostojen kopiointi järjestelmästä tai sisältöoikeuksien hallinnan, IRM:n, avulla. Sisältöoikeuksien hallinnan avulla käyttäjien

voidaan antaa kopioida tiedostot haluamiinsa sijainteihin, mutta tiedostot ovat silti suojattuja ennalta määritetyin säännöin.

IRM käyttää hyväksi Azuren Rights Management -palvelua. Microsoft Azuren kautta yrityksessä voidaan tehdä yrityskohtaisia sääntöjä tiedostojen säilyvyydestä järjestelmän ulkopuolella. Sääntöjen avulla voidaan helposti toteuttaa myös sähköpostiviestien automaattinen salaus halutuissa tilanteissa.

Tieto siitä, kenellä tulisi olla pääsy mihinkin tietoon ja mitä tietoa yrityksen sisältä saa jakaa ulkopuolisille, tulee yrityksen johdon mietittäväksi. Tutkimus osoitti palveluiden olevan siinä tilassa, että jo sisäänrakennetuilla työkaluilla monipuoliset suojaukset ovat toteutettavissa, mutta nämä ominaisuudet tulevat vasta suuryrityksille tarkoitetun Office 365 E3 -palvelutason myötä.

Toisena alakysymyksenä oli:
Kuinka eri mobiilipäätelaitteet toimivat yhdessä palvelujen kanssa?

Tutkimuksessa mukana olleet päätelaitteet: Windows Phone 8.1, Windows RT 8.1, Android-käyttöjärjestelmän puhelin sekä Applen iPad toimivat kaikki ongelmitta palveluiden kanssa. Eroja laitteiden välillä tuli lähinnä eri hallintaominaisuuksien ja sisäänrakennettujen sovellusten osalta. Vaikka verkkoselaimen kautta ohjelmistojen käyttö on lähestulkoon vastaavaa kuin tietokoneilla, on mobiililaitteiden käyttöliittymän vuoksi laitteille tehty omia sähköposti- ja toimistosovelluksia. Uusimpien mobiililaitteiden toimistosovellusversioiden avulla päästään monin paikoin jo lähelle samaa käyttökokemusta kuin tietokoneiden vastaavilla sovelluksilla, jolloin työskentely laitteiden välillä muuttuu hyvin helpoksi. Tietokoneiden ja mobiililaitteiden tehokkaan ja sujuvan yhteiskäytön edellytyksenä voidaan pitää tietojen tallentamista pilvipalveluihin, ei päätelaitteiden omaan muistiin.

Mobiililaitteiden liittäminen palveluihin tapahtuu yrityksessä päätettyjen sääntöjen mukaisesti. Jos yrityksessä on sallittu mobiililaitteen yhdistäminen yrityksen Office 365 -tiliin, Exchange ActiveSync määrittelee liittämisen jälkeen laitteen salasana-

ja salauskäytännöt. Laitteen liittämiseksi Windows Intuneen, käyttäjän tulee asentaa ja kirjautua yritysportaalisovellukseen. Yritysportaalin kautta käyttäjän ladattavaksi voidaan antaa yrityksessä hyväksytyt sovellukset ja ottaa käyttöön edistyneemmät hallintamenetelmät.

Windows 8.1 -käyttöjärjestelmän yleistyessä yrityksissä, esiin tulee uusia hallintamahdollisuuksia Windows Intunen kanssa. Windows 8.1 -käyttöjärjestelmästä johtuen, tietokoneet voidaan tuoda Intunen piiriin myös mobiililaitteina, jolloin myös kadonneen tietokoneen etätyhjennys on mahdollista.

Kolmantena alakysymyksenä oli:
Miten palvelujen saavutettavuus ja jatkuvuus on turvattu?

Microsoft on edelleen, kilpailun kovenemisesta ja toimintaympäristön muutoksesta huolimatta, toimistosovellusten ylivoimainen ykkösnimi. Samoin Microsoftilla on vahva asema yritysten käyttämissä järjestelmissä niin Exchange-sähköpostin, Active Directory -hakemistojen kuin System Center Configuration Managerin hallintaominaisuuksien kautta. Microsoftin pilvipalvelustrategiaan kuuluukin tarjota vastaavat palvelut pelkästään pilvipalveluiden kautta, jolloin palveluihin päästään käsiksi kaikilla päätelaitteilla. Tässä strategiassa Microsoft on mukana tosissaan, mistä kertoo se, että uusi toimitusjohtaja nimitettiin pilvipalveluiden puolelta. Uuden toimitusjohtajan puheessaan julkistama visio ”mobile first, cloud first” kuvastaa hyvin meneillään olevaa muutosta: pilvipalveluiden kehittäminen on Microsoftille elintärkeää. Näiden näkökulmien pohjalta Microsoftin palveluiden jatkuvuudesta tuskin on lähivuosinakaan huolta.

Palveluiden saavutettavuus puolestaan riippuu Internet-yhteydestä ja palveluiden toimivuudesta. Microsoftin lupaus palveluiden saatavuustasosta on 99,9 %. Microsoftin vuosineljänneksittäin julkaisemat toteutuneet käytettävyystasot ovat olleet huomattavasti lupausta parempia ja ovat todennäköisesti paljon parempia, mihin pk-yrityksen omien palvelimien avulla päästäisiin.

Internet-yhteys on pilvitoimintamallissa erityisen tärkeässä asemassa, sillä kaikkia palveluita käytetään verkkoyhteyden kautta. Toisaalta yrityksen kiinteän verkon tärkeyden merkitys pienenee, koska palveluihin päästään käsiksi myös mobiililaitteilla paikasta riippumatta. Riippuvuutta Internet-yhteydestä voidaan vähentää käyttämällä tiedostosynkronointia tärkeimmille työtiedostoille, jolloin työskentelyä voidaan jatkaa myös verkkokatkojen aikana.

Viimeisenä tarkentavana alakysymyksenä oli:
Kuinka turvallisina palveluita voidaan pitää verrattuna oman palvelinsalin ratkaisuihin?

Pilvipalveluiden tietoturvasta ja lähinnä sen puutteesta on puhuttu jo vuosia. Uhkakuvat osin toteutuivat NSA:n vakoilutapauksen paljastumisen myötä. Vakoilutapauksesta huolimatta on syytä muistaa, että valtioiden suorittamaa vakoilua tapahtuu kaikkialla ja suomalaisen pk-yrityksen tiedot tuskin ovat kovin kiinnostavia valtioiden näkökulmasta. Lisäksi vakoilutapaus paljasti NSA:lta löytyvän tekniikkaa, jolla laitteita voidaan vakoilla, vaikka ne eivät olisi kiinni verkossa. Täten voitaneen olettaa valtioiden pystyvän tarvittaessa vakoilemaan haluamaansa kohdetta, joten pk-yrityksen näkökulmasta tärkeämpää on se, miten tieto on suojattu muilta käyttäjiltä.

Tapaus NSA herätti pilvitoimintamallilla toimivat yritykset muuttamaan palveluiden suojauskäytäntöjä. Microsoftin järjestelmään tekemien salauksen parantamisien ja käyttäjien hallittavaksi tuotujen ominaisuuksien hyödyntämisen avulla yrityksen tiedot voidaan nykyisin suojata hyvin eteen tulevia uhkakuvia varalta. Vakoilutapaus näyttääkin kääntyneen kuluttajien voitoksi uusien parannettujen palveluiden myötä.

Microsoft rakentaa luottamusta pilvipalveluitaan kohtaan muun muassa useiden eri tahojen myöntämien sertifikaattien ja auditointien kautta. Näiden avulla asiakas voi varmistua tehtyjen palvelujen turvallisuudesta niin fyysisen kuin myös teknisen toteutuksen osalta. Pilvipalveluiden toteutukset Microsoftin tapauksessa ovatkin

tehty vastaamaan kaikkien yritysten tarpeita, jolloin ratkaisut ovat mitoitettu suuryritysten tarpeisiin. Vastaavan tasoiset oman palvelinympäristön toteutukset eivät ole pk-yrityksen resursseilla käytännössä mahdollisia saati järkeviä toteuttaa, sillä ne vaatisivat paljon resursseja ja laajaa tietämystä eri tekniikoista.

Palvelinten sijainnista ja turvallisuustasoista riippumatta suurimpana riskinä ovat palveluiden käyttäjät. Ihmiset käyttävät varsinkin sähköpostia myös tärkeiden ja arkaluontoisten viestien ja tiedostojen välittämiseen. Tätä kautta sähköpostin käyttäjien ja myös lähetettyjen sähköpostien vastaanottajien sähköpostilaatikot voivat sisältää paljon yritykselle kriittistä tietoa ja aiheuttaa näin ollen vakavan tietoturvauhkan huolimatta siitä, onko tieto pilvipalvelimella vai talon sisällä. Pilvipalveluiden uusien ominaisuuksien käyttöönoton myötä pk-yritys voikin parantaa tietoturvan tasoa läpi organisaation määrittelemällä yritykselle sopivat sisältöoikeuksien käyttösäännöt ja tehokkaat käyttäjien todentamismenetelmät. Näiden toimien määrittämistä tulisikin ajatella osana yrityksen riskienhallintasuunnitelmaa.

5.1 TYÖN TULOSTEN ARVIOINTI

Tämän tutkimuksen päärajaus tehtiin kohdeyrityksen käytössä olevien pilvipalveluiden pohjalta. Työn edetessä havaittiin rajauksen olevan liian laaja, ja sitä täsmennettiin koskemaan palveluiden uusia ominaisuuksia. Rajauksen täsmennyksistä huolimatta pilvipalveluiden uusien ominaisuuksien määrän kasvaminen pelkästään tutkimuksen aikana vaikeutti työn tekemistä. Tutkimus kuitenkin osoitti myös tätä kautta, kuinka tärkeää yrityksissä on seurata uusien ominaisuuksien kehitystä ja testata, soveltuvatko niiden ominaisuudet omaan toimintaan.

Yrityksessä tehtyä vaatimusmäärittelyä tarkasteltiin työssä Windows Intunen ja Office 365:den tuomien ominaisuuksien kannalta (taulukko 10). Jaottelu Intune- ja Office 365 –osioihin muodostui joitakin päällekkäisyyksiä lukuun ottamatta melko luonnollisesti. Mobiililaitteiden hallintaa ja etätoimia laitteille päädyttiin käsittelemään niin Intunen kuin myös Office 365:den osalta. Näiden lisäksi esimerkiksi lisenssien hallintaa tehdään Office-ohjelmistojen osalta Office 365:den puolelta, josta saadaan tarvittaessa myös Office-ohjelmistojen päivitykset. Toisaalta taas

Windows Intunen puolella olisi voitu käsitellä myös yrityksen tietojen suojaamista osana tietoturvamäärityksiä ja valvontaa. Tehdyn jaottelun katsottiin kuitenkin pitävän paikkansa palveluiden pääasiallisten tehtävien mukaisesti jaoteltuna. Kuvatut esimerkkitapaukset kuitenkin osoittavat, että pilvipalveluilla ratkaisua toteutettaessa tulee huomioida kaikkien palveluiden tarjoamat mahdollisuudet ja vaikutukset tehtävälle toteutukselle.

Taulukko 10. Kooste vaatimusmäärittelyjen jaottelusta ratkaisujen hakemiseksi Windows Intunen ja Office 365:den avulla.

Nro	Vaatimus	Yhteinen tekijä
1	Kaikkien tietokoneiden hallinta riippumatta sijainnista	Päätelaitehallinta
4	Mobiililaitteiden hallinta	
2	Tiedot asennetuista ohjelmistoista	Asennetut ohjelmistot
3	Lisenssien hallinta	
8	Etätoimet laitteille	Etätoimet
10	Etätuki	
11	Ohjelmistojen ja päivitysten asennukset	
7	Tietoturvamääritykset ja valvonta	Tietoturva
5	Käyttäjän omien tiedostojen saavutettavuus eri päätelaitteilla	Tiedostoihin pääsy ja tiedon suojaaminen
6	Yrityksen tiedostojen saavutettavuus eri päätelaitteilla	
12	Yrityksen tiedon suojaaminen	
13	Projektien tiedostojen hallinta	
15	Turvallinen sähköpostiliikenne	
4	Mobiililaitteiden hallinta	Mobiililaitteiden hallinta
8	Etätoimet laitteille	
16	Kadonneen salasanan hyödyntämisen havaitseminen	Tietoturva ja palveluiden saavutettavuus
17	Yhteysongelmatilanteisiin varautuminen	

Taulukon värien selitykset:

Windows Intunen avulla ratkaisujen etsintä
Office 365:den avulla ratkaisujen etsintä
Intune + Office 365:den avulla ratkaisujen etsintä

Tutkimusympäristön myötä työssä tuli selkeästi esille Microsoft Azuren tärkeä rooli palveluiden taustalla. Azure on Office 365:den kanssa oleellinen apuväline otettaessa käyttöön uusia tehokkaampia suojausmekanismeja. Myös Office 365 palvelupaketin valinnalla on suuri merkitys mitä suojauksia pystytään toteuttamaan. Tutkimus kuitenkin osoitti että Microsoftin pilvipalveluilla on mahdollista toteuttaa hyvinkin tehokkaita suojausominaisuuksia pk-yrityksen tiedonhallintaan ja kaikkien päätelaitteiden hallitsemiseksi. Tiedon sekä päätelaitteiden suojaamisessa on kuitenkin hyvä muistaa, mitä tietoa halutaan suojata ja kuinka tämä vaikuttaa palveluiden käytettävyyteen. Yrityksen kriittinen tieto tulee toki suojata aina mahdollisimman hyvin, mutta perustiedostojen suojauksen kohdalla kannattaa asiaa tarkastella tapauskohtaisesti. Tulisi löytää sopiva keskitie käytettävyyden ja suojauksen väliltä, jotta käyttäjät eivät hylkää yrityksen järjestelmiä liian vaikean käytettävyyden vuoksi.

Tutkittaessa Microsoft Azuren ominaisuuksia, heräsi mielenkiinto tutkia myös yrityksen palvelimien siirtämistä Azureen, jolloin yrityksen kaikki toiminta tapahtuisi pilvipalveluiden avulla. Tämä voisikin olla yrityksessä jatkotutkimuksen paikka, jolla päästäisiin hyödyntämään aina uusinta tekniikkaa myös palvelimissa. Samalla yritys voisi saada säästöjä edullisempien kuukausimaksujen kautta, mutta myös uusien palveluiden perustamisen nopeuden ja paremman mitoituksen myötä.

6 JOHTOPÄÄTÖKSET

Pilvipalvelujen päivitystahti on nykyisin hyvin nopea. Perinteisten ohjelmistojen käytössä on totuttu jopa useamman vuoden päivitysväleihin, kun taas pilvipalveluiden ominaisuuksiin tulee päivityksiä joka vuosineljännes. Suurin syy siihen, että kohdeyritys halusi tämän tutkimuksen tehtäväksi, oli juurikin palveluiden tiivis päivitystahti – niihin haluttiin perehtyä rauhassa tarkemmin. Yrityksessä haluttiin saada selville palveluiden tämänhetkiset mahdollisuudet yrityksen tietojen turvalliseen hallintaan niin yritysdatan kuin myös päätelaitteiden suojauksen kannalta.

Yrityksen päätökseen siirtää toimintojaan pilvipalveluihin vaikuttaa luottamus palveluntarjoajaan, palvelun tietoturvallisuus, luotettavuus ja vaatimusten mukainen toteutus. Näiden todistamiseksi pilvipalveluita tarjoavat yritykset pyrkivät mahdollisimman läpinäkyvään toimintaan niiltä osin kuin se pilvipalveluissa on mahdollista. Lisäksi yritykset käyttävät kolmannen osapuolen todentamia sertifikaatteja ja muita hyväksyntöjä luodessaan luottamusta mahdolliseen asiakaskuntaansa.

Luottamus pilvipalveluihin kuitenkin järkkyi kesällä 2013 paljastuneen NSA:n vakoilutapauksen myötä. Pilvitoimintamallin yrityksissä tapaus sai aikaan laajojen toimenpiteiden aallon, jolla palvelut pyrkivät saamaan takaisin menetettyä luottamusta pilvipalveluitaan kohtaan. Myös Microsoft paransi pilvipalveluiden salausta ja tiedonsuojauksen menetelmiä. Microsoftin pilvipalvelut ovatkin kehittyneet suurin harppauksin viimeisen vuoden aikana. Nykyisillä palveluilla on mahdollista kytkeä päälle hyvinkin tehokkaita tiedon suojaamisen menetelmiä, ja tieto pysyy salattuna niin palveluiden sisällä kuin myös siirtämisen aikana.

Microsoft totesi Office 365:den teknisessä turvallisuusdokumentissaan turvallisuuden kehittämisen olevan jatkuva prosessi. Tämän lauseen paikkansapitävyys on tullut esiin monesti tämän diplomityön kirjoittamisen aikana, ja lainattujen lähteiden tiedot vanhenevat nopeasti. Tämä uusien ominaisuuksien lisääminen palveluun on toki hyvä asia, mutta tarkoittaa yrityksen IT-henkilöstön kannalta jatkuvaa omien

tietojen päivittämisen tarvetta. Yrityksissä olisikin syytä pysähtyä aika ajoin arvioimaan uusien ominaisuuksien käyttöönoton tarvetta ja sitä, mitä hyötyjä uusien toteutuksien avulla saavutettaisiin.

Lähdeluettelo

[1] Elisa Oyj, ”Tuotekehityksen historia,” 2014. [Online]. Saatavissa: http://corporate.elisa.fi/elisa-oyj/elisa-oyj/historia/tuotekehityksen-historia/. [Haettu 12.3.2014].

[2] Microsoft, ”Empowering People-Centric IT,” 2013. [Online]. Saatavissa: http://download.microsoft.com/download/7/1/9/719DE128-E02B-408E-BCC1-CC45AA0538AB/enabling_people_centric_IT_preview_guide.pdf. [Haettu 8.3.2014].

[3] E. Naone, ”Technology overview - Conjuring Clouds,” *Technology Review*, osa/vuosik. 112, nro 4, pp. 54 - 56, 2009.

[4] J. Voas ja J. Zhang, ”Cloud Computing: New Wine or Just a New Bottle?,” *IT Professional*, osa/vuosik. 11, nro 2, pp. 15 - 17, 2009.

[5] Gartner Inc., ”Gartner says two-thirds of enterprises will adopt a mobile device management solution for corporate liable users trough 2017,” 2012. [Online]. Saatavissa: http://www.gartner.com/newsroom/id/2213115. [Haettu 11.2.2014].

[6] Gartner Inc., ”Gartner says cloud office systems total 8 percent of the overall office market and will rise to 33 percent by 2017,” 2013. [Online]. Saatavissa: http://www.gartner.com/newsroom/id/2514915. [Haettu 17.7.2013].

[7] D. Michael, N. Aggarwal, D. Kennedy, J. Wenstrup, M. Rübmann, R. Borno, J. Chen ja J. Bezerra, ”Ahead of the Curve - Lessons on Technology and Growth from Small-Business Leaders,” 2013. [Online]. Saatavissa: https://www.bcgperspectives.com/content/articles/technology_software_globalization_ahead_curve_lessons_technology_growth_small_business_leaders/. [Haettu 8.3.2014].

[8] K. M. Khan ja Q. Malluhi, ”Establishing trust in cloud computing,” *IT professional*, osa/vuosik. 12, nro 5, pp. 20 - 27, Syyskuu/Lokakuu 2010.

[9] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang ja A. Ghalsasi, ”Cloud computing - The business perspective,” *Decision Support Systems*, osa/vuosik. 51, nro 1, pp. 176 - 189, 2011.

[10] P. Heino, Pilvipalvelut, Hämeenlinna: Talentum Media Oy, 2010.

[11] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica ja M. Zaharia, ”A view of cloud computing,” *Communications of the ACM*, osa/vuosik. 53, nro 4, pp. 50 - 58, 2010.

[12] P. Mell ja T. Grance, ”The NIST definition of cloud computing,” Special Publication 800.145, Heinäkuu 2011. [Online]. Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. [Haettu 25.7.2013].

[13] R. Clarke, ”How reliable is cloudsourcing? A review of articles in the technical media 2005 - 11,” *Computer Law & Security Review*, nro 28, pp. 90 - 95, 2012.

[14] B. Kepes, ”Understanding the cloud computing stack: PaaS, SaaS, IaaS.,” 2013. [Online]. Saatavissa: http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas. [Haettu 12.3.2014].

[15] R. Alirezaei, B. Scwartz, M. Ranlett, S. Hillier, B. Wilson, J. Fried ja P. Swider, Professional Sharepoint 2013 Development, Indianapolis: John Wiley & Sons, Inc., 2013, p. 788.

[16] R. L. Krutz ja R. D. Vines, Cloud security: A comprehensive guide to secure cloud computing, John Wiley & Sons, 2010, p. 384.

[17] D. Zissis ja D. Lekkas, ”Addressing cloud computing security issues,” *Future generation computer systems,* osa/vuosik. 28, nro 3, pp. 583 - 592, 2012.

[18] Nixu Oy, ”Kännykkäsovellukset: Älä asenna mitä hyvänsä,” 2014. [Online]. Saatavissa: http://nixu.com/fi/julkaisut/kannykkasovellukset-ala-asenna-mita-hyvansa. [Haettu 14.3.2014].

[19] J. Huang ja D. M. Nicol, ”Trust mechanisms for cloud computing,” *Journal of cloud computing,* osa/vuosik. 2, nro 1, pp. 1 - 14, 2013.

[20] A. Skendzic ja B. Kovacic, ”Microsoft Office 365 - cloud in business environment,” tekijä: *MIPRO, 2012 Proceedings of the 35th International Convention*, Opatija, 2012.

[21] G. Greenwald ja E. MacAskill, ”NSA Prism program taps in to user data of Apple, Google and others,” *The Guardian,* 7.6.2013.

[22] B. Kiefer, ”Privacy post-PRISM,” *PRWeek,* pp. 26 - 27, Lokakuu 2013.

[23] D. Castro, ”How much will PRISM cost the U.S. cloud computing industry?,” *The Information Technology & Innovation Foundation,* pp. 1 - 9, 2013.

[24] C. Timberg, B. Gellman ja A. Soltani, ”Microsoft. suspecting NSA spying, to ramp up efforts to encrypt its Internet traffic,” The Washington Post, 27.11.2013. [Online]. Saatavissa: http://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story.html. [Haettu 14.3.2014].

[25] B. Smith, ”Protecting customer data from government snooping,” The Official Microsoft Blog, 4.12.2013. [Online]. Saatavissa: http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx. [Haettu 13.3.2014].

[26] A. Wieland, ”Email in the cloud: the challenges and benefits,” *Computer Fraud & Security,* nro 7, pp. 10 - 12, 2012.

[27] S. Dhouib ja B. Halima, ”Surveying Collaborative and Content Management Platforms for Enterprise,” tekijä: *Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2013.

[28] J. Newton, ”Next-Generation ECM,” *KM World,* osa/vuosik. 22, nro 3, pp. 9 - 9, 2013.

[29] Net Market Share, ”Desktop Top Operating System Share Trend,” Market Share Statistics for Internet Technologies, 2014. [Online]. Saatavissa: http://www.netmarketshare.com/?source=NASite. [Haettu 11.3.2014].

[30] Google, ”Google Announces Google Docs & Spreadsheets,” News from Google, 2006. [Online]. Saatavissa: http://googlepress.blogspot.fi/2006/10/google-announces-google-docs_11.html. [Haettu 11.3.2014].

[31] B. Rigby ja A. Oreskovic, ”Microsoft updates Office, vies online with Google,” Reuters, 2010. [Online]. Saatavissa: http://www.reuters.com/article/2010/05/11/us-microsoft-office-idUSTRE64A6JM20100511. [Haettu 11.3.2014].

[32] L. Tung, ”Microsoft squares up to Google in the schoolyard with free Office 365 for students deal,” Zdnet.com, 2013. [Online]. Saatavissa: http://www.zdnet.com/microsoft-squares-up-to-google-in-the-school-yard-with-free-office-365-for-students-deal-7000023873/. [Haettu 11.3.2014].

[33] Microsoft, ”Satya Nadella - Chief Executive Officer,” News Center, 2014. [Online]. Saatavissa: http://www.microsoft.com/en-us/news/exec/nadella/. [Haettu 11.3.2014].

[34] S. Nadella, ”Mobile First, Cloud First Press Briefing,” Microsoft News Center, 2014. [Online]. Saatavissa: http://www.microsoft.com/en-us/news/speeches/2014/03-27nadella.aspx. [Haettu 2.6.2014].

[35] Microsoft, ”Microsoft Unveils Windows Azure at Professional Developers Conference,” News Center, 2008. [Online]. Saatavissa: https://www.microsoft.com/en-us/news/press/2008/oct08/10-27pdcday1pr.aspx. [Haettu 2.6.2014].

[36] Microsoft, ”Windows Azure,” Documentation, 2014. [Online]. Saatavissa: https://www.windowsazure.com/en-us/documentation/. [Haettu 30.3.2014].

[37] Microsoft, ”Windows Azure Trust Center,” 2014. [Online]. Saatavissa: http://www.windowsazure.com/en-us/support/trust-center/. [Haettu 30.3.2014].

[38] Gartner Inc., ”Magic Quadrant for Cloud Infrastructure as a Service,” 2014. [Online]. Saatavissa: http://www.gartner.com/technology/reprints.do?id=1-1UM941C&ct=140529&st=sb. [Haettu 2.6.2014].

[39] M. Katzer ja D. Crawford, Office 365: Migrating and managing your business in the cloud, Apress, 2013.

[40] Microsoft, ”Vertaa yritysten Office 365 -palvelupaketteja,” Office tuotteet, 2014. [Online]. Saatavissa: http://office.microsoft.com/fi-fi/business/vertaa-kaikkia-yrityksille-tarkoitettuja-office-365-palvelupaketteja-FX104051403.aspx. [Haettu 12.7.2014].

[41] Microsoft, ”Office on Demandin käyttäminen,” Office tuki, 2014. [Online]. Saatavissa: http://office.microsoft.com/fi-fi/office365-suite-help/office-on-demandin-kayttaminen-HA103337813.aspx. [Haettu 4.4.2014].

[42] M. R. Gilbert, K. M. Shegda, K. Chin, K. Tay ja H. Koehler-Kruener, ”Magic Quadrant for Enterprise Content Management,” Gartner Inc., 2013. [Online]. Saatavissa:

http://www.collectiveintelligence.com/Solutions/Web-Portals/Documents/Gartner-Magic%20Quadrant%20for%20Enterprise%20Content%20Management.pdf. [Haettu 8.3.2014].

[43] L. Low, ”Sharepoint 2010,” *Technet magazine,* pp. 22-24, Huhtikuu 2011.

[44] Microsoft, ”Sharepoint Online,” Office Products, 2014. [Online]. Saatavissa: http://office.microsoft.com/en-us/sharepoint/microsoft-sharepoint-online-collaboration-and-management-software-FX103789366.aspx. [Haettu 2.6.2014].

[45] Microsoft, ”Lync server 2013,” Office tuotteet, 2014. [Online]. Saatavissa: http://office.microsoft.com/fi-fi/lync/lync-server-2013-ominaisuudet-videoneuvottelut-ja-pikaviestit-FX103789571.aspx. [Haettu 2.6.2014].

[46] Microsoft, ”Mikä on OneDrive for Business?,” Office tuki, 2014. [Online]. Saatavissa: http://office.microsoft.com/fi-fi/sharepoint-server-help/mika-on-onedrive-for-business-HA102822076.aspx. [Haettu 23.7.2014].

[47] J. Pohjala, ”Työasemien hallinta ja käyttöjärjestelmä pilvestä - Windows Intune julkaistu,” Microsoft TechNet Finland IT Pros Blog, 2011. [Online]. Saatavissa: http://blogs.technet.com/b/fiitpro/archive/2011/03/24/ty-246-asemien-hallinta-ja-k-228-ytt-246-j-228-rjestelm-228-pilvest-228-windows-intune-julkaistu.aspx. [Haettu 22.7.2014].

[48] Microsoft, ”Documentation Library for Windows Intune,” Technet, 2014. [Online]. Saatavissa: http://technet.microsoft.com/en-us/library/jj676587.aspx. [Haettu 24.7.2014].

[49] Microsoft, ”Windows Intune Service Description,” Technet, 2014. [Online]. Saatavissa: http://technet.microsoft.com/en-us/library/dn600286.aspx. [Haettu 2.6.2014].

[50] Microsoft , ”Windows Intune Service Updates,” Technet, 2014. [Online]. Saatavissa: http://technet.microsoft.com/en-us/library/dn292747.aspx#bkmk_ape. [Haettu 15.6.2014].

[51] Microsoft, ”Windows 7 Enterprise,” Windows - Tuotteet ja teknologiat, 2014. [Online]. Saatavissa: http://www.microsoft.com/fi-fi/windows/enterprise/windows7.aspx. [Haettu 3.6.2014].

[52] Microsoft, ”Security in Office 365 Whitepaper,” Microsoft Download Center, 2013. [Online]. Saatavissa: http://www.microsoft.com/en-us/download/details.aspx?id=26552. [Haettu 8.3.2014].

[53] J. Meisner, ”Protecting customer data from government snooping,” Microsoft, 2013. [Online]. Saatavissa: http://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/. [Haettu 12.5.2014].

[54] Microsoft, ”Security and Compliance Office 365,” Toukokuu 2014. [Online]. Saatavissa: http://office.microsoft.com/en-us/business/redir/XT104030898.aspx. [Haettu 5.6.2014].

[55] Microsoft, ”The Office 365 Trust Center,” 2014. [Online]. Saatavissa: http://office.microsoft.com/en-us/business/redir/XT104030898.aspx. [Haettu 4.6.2014].

[56] Microsoft, ”Azure Multi-Factor Authentication,” Technet, 2013. [Online]. Saatavissa: http://technet.microsoft.com/library/en-us/dn249471. [Haettu 21.4.2014].

[57] Microsoft, ”Introducing Office 365 Message Encryption: Send encrypted emails to anyone!,” Office Blogs, 2013. [Online]. Saatavissa: http://blogs.office.com/2013/11/21/introducing-office-365-message-encryption-send-encrypted-emails-to-anyone/. [Haettu 17.4.2014].

[58] Microsoft, ”Office 365 Message Encryption,” Technet, 2014. [Online]. Saatavissa: http://technet.microsoft.com/en-US/library/dn569286.aspx. [Haettu 16.4.2014].

[59] Microsoft, ”SharePoint Online: ohjelmistojen rajat ja rajoitukset,” Office tuki, [Online]. Saatavissa: http://office.microsoft.com/fi-fi/office365-sharepoint-online-enterprise-help/sharepoint-online-ohjelmiston-rajat-ja-rajoitukset-HA102694293.aspx. [Haettu 22.6.2014].

[60] P. Andrew, ”Multi-Factor Authentication for Office 365,” Microsoft, 2014. [Online]. Saatavissa: http://blogs.office.com/2014/02/10/multi-factor-authentication-for-office-365/. [Haettu 6.5.2014].

[61] D. Wlodarz, ”Comparing cloud vs on-premise? Six hidden costs people always forget about,” Betanews, 2013. [Online]. Saatavissa: http://betanews.com/2013/11/04/comparing-cloud-vs-on-premise-six-hidden-costs-people-always-forget-about/. [Haettu 6.7.2014].

LIITTEET

Liite 1. Yrityksen laatima vaatimusmäärittely pilvipohjaisille toimisto- ja hallintasovelluksille

Tunnus	Vaatimus	Tärkeys	Perustelu	Nykyinen ratkaisu / Mahdollinen uusi ratkaisu
1	Kaikkien yritysten tietokoneiden hallinta riippumatta sijainnista	1	Työmaat irrallaan yrityksen kiinteästä toimipisteverkosta	Windows Intune / Windows Intune
2	Tiedot asennetuista ohjelmistoista ja niiden versioista	2	Tietokoneet hankittu ajan mittaan, joten eri versioita sovelluksista	Windows Intune / Windows Intune
3	Lisenssien hallinta järjestelmän avulla	2	Tiedot lisenssinvaraisista ohjelmista ja niiden asennuksista tulisi saada muualta kuin excel tiedostoista	Windows Intune ja Excel / Windows Intune
4	Mobiililaitteiden hallinta	1	Mobiililaitteilla nykyisin pääsy moneen paikkaan, joten suojaamiseen kiinnitettävä huomiota	Office 365 exchange / Windows Intune + O365
5	Käyttäjän tiedostot käytettävissä kaikilla päätelaitteilla	2	Toimittaessa useilla päätelaitteilla, käyttäjän työtiedostot tulisi olla aina käytettävissä	Office 365:den kautta tulevat OneDrive for Business sekä SharePoint
6	Yrityksen yhteiset tiedostot saavutettavissa kaikilla päätelaitteilla	2	Toimintajärjestelmän dokumentit ja työmaiden lomakemallit tulisi olla saavutettavissa kaikkialta.	Käyttäjien omat tietokoneet ja SharePoint työryhmätilat / SharePointin työryhmätilat
7	Tietoturvan valvonta ja määritykset	1	Koneiden hälytyksistä täytyy saada tieto IT:lle pikaisesti. IT asettaa tietoturvamääritykset, joita käyttäjä ei voi ohittaa	Windows Intune ja osin F-Securen PSB / Windows Intune ja automaattiset hälytykset käyttöön. Käyttäjillä ei saa olla pääkäyttäjätunnuksia koneelleen.
8	Etätoimet laitteille esim. katoamistapauksessa	1	Matkapuhelimet exchangen avulla, mutta miten tietokoneet?	Office 365 Exchange matkapuhelimissa, tietokoneissa ei mitään / Windows Intunen avulla saadaan puhelimet etälukittua tai tyhjennettyä. Tietokoneista etänä voidaan poistaa joitakin ohjelmia, mutta kokonaan tyhjennystä ei voida tehdä. Tämä vaatisi jonkin kolmannen osapuolen ratkaisun.
9	Tiedon suojaaminen koneen kovalevyllä	1	Kadonneen tietokoneen tiedot helppo lukea suojaamattomalta kovalevyltä	Pieni osa koneista salattuja / Bitlocker asemansalaus käyttöön läpi organisaation, jolloin tietoja ei saada luettua irrotetulta kovalevyltä.
10	Käyttäjätuki etäyhteyden avulla	3	Nykyinen ohjelmisto toimii hyvin, mutta mahdollisuus säästöihin jos järjestelmän sisällä tuki etäyhteyksille	Windows Intunen Easy assist voisi olla ratkaisu, mutta ei toimi

Tunnus	Vaatimus	Tärkeys	Perustelu	Nykyinen ratkaisu / Mahdollinen uusi ratkaisu
				tällä hetkellä Windows 8.1:n kanssa.
11	Ohjelmistojen asennukset ja päivitykset	2	Uusien ohjelmistojen ja päivitysten jakelu hajallaan olevalle laitekannalle haasteellista	Windows Intune / Windows Intune automatisoiduilla kriittisten päivitysten asennuksella
12	Yrityksen datan suojaaminen	1	Kriittisen datan täytyy pysyä talon sisällä	SharePointissa ja sähköpostissa olevat tiedostot suojattu vain salasanoilla / Office 365 sääntöjen avulla voidaan hallita koneelle tallennettavia, tulostettavia ja uloslähetettäviä tiedostoja.
13	Projektien tiedostojen jako ja arkistointi	3	Nykyisin käytössä erillisiä projektipankkeja	Tietokoneiden kiintolevyt ja projektipankit / Erilliset projektipankit voitaisiin korvata SharePointin työryhmätiloilla
14	Yhdet kirjautumistunnukset	2	Kirjautumistunnus tietokoneeseen ja palveluihin tulisi olla sama	Ei toteutettu / Vaatii Active Directory synkronoinnin. Active Directory voi sijaita myöskin pilvessä Azuren päällä
15	Turvallinen sähköpostiliikenne	1	Sähköpostiliikenteen turvaaminen myös yleisissä verkoissa	O365 / Office 365 sähköpostiliikenne käyttää salattua yhteyttä kaikkialla. Lisäksi tulossa mahdollisuus helppoon viestien salaukseen
16	Mahdollisesti hukkuneen salasanan hyödyntämisen havaitseminen	2	webmail kirjautuminen mahdollistaa kirjautumisen kaikilta laitteilta, joten asiattomien kirjautuminen järjestelmään tulisi estää	Ei tutkittu / Azuren WAAD ja kehittyneemmät raportointiominaisuudet sekä monivaiheinen todentaminen tuntemattomalta tietokoneelta/ laitteelta
17	Yhteysongelmatilanteissa toiminnan jatkuminen	1	Yrityksellä tulee olla pääsy tärkeisiin dokumentteihin myös mahdollisen verkko-ongelman aikana	Puhelimet toimivat varayhteytenä / Tärkeää että toimistolla on jokin varayhteys Internetiin, esim. älypuhelimen verkko. Jos palvelu on poissa käytöstä, voidaan käyttää tietokoneen muistissa olevia sähköposteja ja Offline tiedostoiksi määritettyjä SharePoint kansioita

Liite 2. Office 365:den tilauspakettien vertailua. [40]

	Small Business	Small Business Premium	Midsize Business	Sähköposti Exchange Online	Enterprise E1	Enterprise E3	Enterprise E4
Hinta/ käyttäjä/kk	4,10 €	10,40 €	12,30 €	3,30 €	6,50 €	19,00 €	20,90 €
Käyttäjien enimmäismäärä	25 käyttäjää	25 käyttäjää	300	Rajoittamaton	Rajoittamaton	Rajoittamaton	Rajoittamaton
Office-työpöytäsovellukset		x	x			x	x
Isännöity sähköposti (50Gt)	x	x	x	x	x	x	x
Verkkoneuvottelut, tavoitettavuustiedot ja pikaviestit	x	x	x		x	x	x
1 Tt henkilökohtaista tallennustilaa kullekin OneDrive for Business –käyttäjälle	x	x	x		x	x	x
Julkinen sivusto	x	x	x		x	x	x
Suojaus roskapostilta ja haittaohjelmilta	x	x	x	x	x	x	x
Yhteisö- ja puhelintuki 24/7	x	x	x	x	x	x	x
99,9 %:n käyttöaste, hyvityksiin perustuva palvelutasosopimus (SLA).	x	x	x	x	x	x	x
SharePoint-sivustot	x	x	x		x	x	x
Office Online tiedostojen luomiseen ja muokkaukseen selaimella	x	x	x	Vain liitteiden tarkastelu	x	x	x
Sivustopostilaatikot		x	x		x	x	x
Active Directory –integrointi			x	x	x	x	x
Mobiilisovellukset iPadissa sekä iPhone-, Android- ja Windows Phone puhelimissa		x	x			x	x
Yammer Enterprise			x		x	x	x
Kehittyneet sähköpostiominaisuudet						x	x
eDiscovery Center velvoitteiden noudattamisen seurantaan						x	x
Kehittyneet ääniominaisuudet						x	x
Omatoiminen liiketoimintatietojen hallinta			x			x	x
Yrityksen puheluratkaisu							x