LAUREA

TIETOTURVAN KEHITTÄMINEN SÄHKÖPOSTILIIKENTEESSÄ

Saarinen, Ville

2013 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tietoturvan kehittäminen sähköpostiliikenteessä

Saarinen, Ville
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Tammikuu, 2013

Laurea-ammattikorkeakoulu
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Tiivistelmä

Saarinen, Ville

Tietoturvan kehittäminen sähköpostiliikenteessä

Vuosi 2013 sivumäärä 36

Sähköposti on nykypäivänä yksi keskeisimmistä viestintämuodoista. Sähköpostin turvallinen käyttö on kuitenkin riippuvainen toimivasta tietoturvasta. Sähköpostin vaivattomuus ja helppokäyttöisyys voi menettää merkityksensä kokonaan huonon tietoturvan vuoksi.

Opinnäytetyön aiheena on tutkia tietoturvahaavoittuvuutta yrityksen sähköpostijärjestelmässä. Työ on case- tutkimus ja sen tarkoituksena on tutkia erilaisia menetelmiä tietoturva-aukon paikkaamiseksi ja tarjota näistä menetelmistä parhaiten toimiva ratkaisu. Opinnäytetyössä käsitellään aiheeseen liittyvät käsitteet, kuten VPN, digitaalinen sertifikaatti, tietoturva-aukko ja sähköpostipalvelin.

Tietoturva-aukon paikkaaminen tutkittiin jokaisen ratkaisumenetelmän kanssa teoreettisesti. Yksi menetelmä valittiin tarkempaan tutkintaan ja toteutus kuvattiin eri menetelmillä. Näistä menetelmistä yksi valittiin toimivuuden, resurssikulujen ja hyöty- ja haittaperusteluin ratkaisuksi tietoturvaongelmaan.

Asiasanat VPN, digitaalinen sertifikaatti, tietoturva-aukko, sähköpostipalvelin.

University of Applied Sciences
Laurea Leppävaara
Bachelor's Degree Programme in Business Information Technology

Abstract

Saarinen, Ville

Improving the security of email traffic

Year 2013 pages 36

Email is one of the most used means of communication. However, safe use of email depends on efficient information security. Easy and user friendly email can lose its purpose entirely because of low security.

The subject of the thesis is to examine information security vulnerability in an email system. It is a case study which will be implemented to a certain company. The purpose is to study different solutions to the security vulnerability and to offer the best available solution. Various types of subjects are discussed in the thesis, such as VPN (virtual private network), digital certificate, security vulnerability and email server.

The solutions to the security vulnerability were examined theoretically. One of the solutions was chosen for closer examination and the implementation was described with different techniques. One of these techniques was chosen, with the criteria of functionality, budget and adverse benefit, as a solution to the security vulnerability.

Key words Virtual private network, digital certificate, security vulnerability, email server

Sisällysluettelo

1 Johdanto

Tietoturva on aina ollut tärkeässä roolissa yritysmaailmassa. Tiedonsiirron ja säilytyksen siirtyessä yhä suuremmaksi osaksi sähköiseen muotoon, astuu esiin uusia haasteita tietoturvan säilyttämiseksi. Jo pienikin epäkohta järjestelmässä voi aiheuttaa suuren haavoittuvuuden, jonka seuraukset voivat olla katastrofaalisia yrityksen toiminnalle. ”Tietoturvallisuus on kiinteä ja keskeinen osa liiketoimintaa, ja liiketoiminta on nykyisin hyvin sidoksissa tietojärjestelmiin. Organisaation tehokkuus, toimivuus ja kehityskyky ovat yleensä osittain tai merkittävästi riippuvaisia tietojärjestelmistä ja niiden tietoturvallisuudesta.” (Laaksonen, Nevasalo & Tomula 2006, 19)

Tietoturva koostuu kolmesta osa-alueesta: Tiedon luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Luottamuksellisuus tarkoittaa tietoa, johon vain asiaankuuluvat ja oikeudet omaavat henkilöt pääsevät käsiksi. Eheydellä tarkoitetaan tiedon ”aitoutta” ja varmuutta siitä, että tieto on oikeaa ja toimivaa. Saatavuudella tarkoitetaan taas tiedon saatavuuden varmistamista ja yhteyden turvaamista. (Järvinen 2002, 22-24)

Tietoturva voidaan kuvastaa ja jakaa eri tavoilla. Petteri Järvinen (2002, 112-113) jakaa yrityksen tietoturvan seuraaviin osa-alueisiin: Hallinnollinen turvallisuus, Henkilöturvallisuus, toimitilaturvallisuus, tietojenkäsittelyn turvallisuus, tietoliikenteen turvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, käyttötoimintojen turvallisuus, tietoaineistoturvallisuus ja yksityisyyden suojaus. ISF (Information Security Forum) jakaa tuotoksessaan ”Standard of Good Practice for Information Security” tietoturvan seuraaviin osiin: Tietoturvallisuuden hallinta organisaatiotasolla, liiketoimintakriittiset järjestelmät, tietojärjestelmät, tietoverkot ja järjestelmäkehitys (Laaksonen, Nevasalo & Tomula 2006, 91).

Sähköposti on nykypäivänä yksi keskeisimmistä viestintämuodoista, niin vapaa-aikana kuin yritysmaailmassakin. Internetin käyttäjistä arviolta kolme neljäsosaa käyttää aktiivisesti sähköpostia (Haasio, Rauhala 2002, 9). Sähköpostin yleistymisen myötä myös tietoturvaa on jouduttu parantamaan. Monella sähköposti on päivittäisessä käytössä, mutta kuinka moni ymmärtää painaessaan lähetä- nappia, mitä viestille oikeasti tapahtuu?

Opinnäytetyön aiheena on sähköpostiliikenteessä ilmenevän tietoturvaongelman tutkiminen ja paikkaaminen. Opinnäytetyön aihe sovittiin yhdessä kohdeyrityksen kanssa. Yhteyshenkilönä toimii yrityksen ICT-manageri, Henkilö X. Intimiteettisuojan vuoksi yritys ei halua paljastaa yrityksen tai yhteyshenkilön nimeä. Työ kohdistuu tietoturvan osalta vain sen teknisiin osa-alueesiin, eikä käsittele tietoturvaan liittyviä inhimillisiä tekijöitä.

Aion tutkia jo olemassa olevia, toimivia vaihtoehtoja tämän aukon paikkaamiseen. Näistä ratkaisuista otan yhden syvempään käsittelyyn ja teen analyysin parhaimman ratkaisun teoreettisesta käyttöönotosta eri menetelmillä.

Tämän työn tarkoituksena on rajata parhaimmat vaihtoehdot tietoturvaongelman paikkaamiseen ja osoittaa yhden ratkaisun käytännön toimivuuden. Vaihtoehdot on valittu olemassa olevan tiedon, sekä yrityksen antamien kriteerien perusteella. Lopputuloksen perusteella aion suositella yritykselle parhaiten sopivaa ratkaisua tietoturvaongelmaan.

1.1 Sanasto

- Tietoturvahaavoittuvuus
  Vika tai heikkous organisaation tietojärjestelmän suunnittelussa, käyttöönotossa tai käytössä, jota hyväksikäyttämällä voidaan vahingoittaa tietojärjestelmää.

- Toiminimi
  toiminimi, eli domain name on yritykselle luotu julkinen tunniste.

- VPN site-to-site tunneli
  Site-to-site VPN tunnelointi on kahden palomuurin/VPn konsentraattorin välinen jatkuva virtuaalinen yksityisverkko, joka mahdollistaa tiedonsiirron suojatussa verkossa julkisen verkon läpi.

- Pilvipalvelu (Cloud service)
  Pilvipalvelu tarkoittaa palveluita, jotka ovat yrityksellä käytössä, mutta eivät sijaitse yrityksellä fyysisesti paikan päällä, vaan ovat sen sijaan kolmannen osapuolen ylläpidettävänä.

- SSL sertifikaatti
  Secure Sockets Layer- tasolla toimiva sertifikaatti. Perustuu julkisen ja symmetrisen avaimen salaukseen.

- IPSEC protokolla
  (IP Security Architecture)- protokolla on joukko internet-yhteyksiä suojaava tietoliikenneprotokolla.

- SLA
  Service Level Agreement, eli palvelutasosopimus on asiakkaan ja palvelutarjoajan välinen sopimus jossa määritellään palvelun taso, sekä palveluntason rajan alittamisen sanktiot.

- Single sign-on

  Single sign-on (SSO) on autentikointimenetelmä, joka mahdollistaa monen yksittäisen ohjelman kirjautumisen samanaikaisesti.

1.2 Case Yritys X

Yritys X on maailman johtava merenkulkualan ohjelmistokehittäjä. Se tarjoaa erilaisia turvallisuus-, logistiikka- ja navigointiratkaisuja laivayhtiöille sekä telakoille. Yrityksen Asiakkaihin kuuluu monet suuret laivayhtiöt ja telakat ympäri maailmaa. Suurin osa telakoista sijaitsee nykyisin Kaukoidässä, ja kuuluvat maailman suurimpiin telakoihin. Varustamoita sen sijaan löytyy ympäri maailmaa.

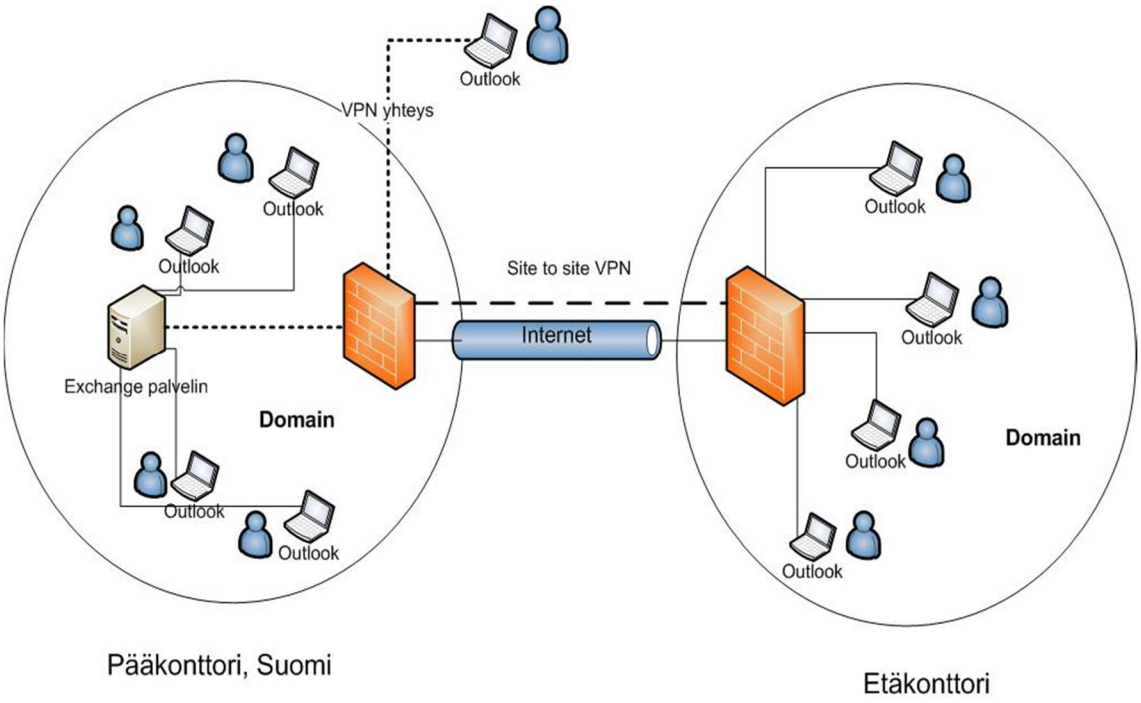
Yrityksen pääkonttori sijaitsee Helsingissä, mutta sillä on myös monia etäkonttoreita muun muassa Kiinassa, Koreassa, Japanissa, Romaniassa, Yhdysvalloissa, Intiassa ja Singaporessa. Napalla on 150 työntekijöitä, joista noin 100 työskentelee Helsingissä. Aasian etäkonttoreiden työntekijät jakautuvat seitsemään työntekijään Kiinassa, neljään työntekijään Japanissa ja kuuteen työntekijään Koreassa.

1.3 Tutkimusongelma

Yrityksen työntekijöillä on käytössä Microsoft Office 2010 Professional Plus- ohjelmat, jonka mukana käyttöön on tullut Outlook 2010- asiakasohjelma. Työntekijöiden työasemat ovat sekä kannettavia, että pöytäkoneita. Työasemat ovat muutamia poikkeuksia lukuunottamatta vakioitu Windows 7 Ultimate käyttöjärjestelmiin.

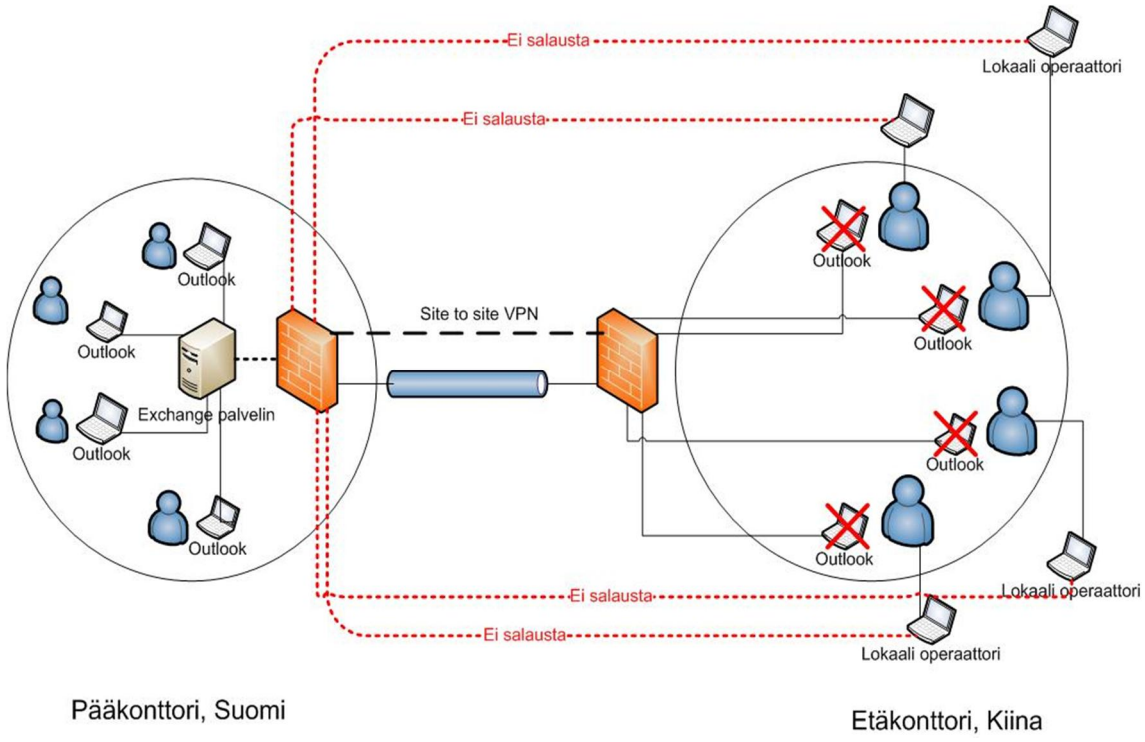
Yrityksellä on käytössä Microsoft Exchange- sähköpostipalvelin, joka sijaitsee yrityksen pääkonttorissa, Helsingissä. Yrityksen työntekijät ottavat Outlook- asiakasohjelmalla yhteyden palvelimella sijaitseviin sähköpostilaatikoihin. Asiakasohjelmien ja palvelimen välillä on reaaliaikainen yhteys, sujuvan sähköisen viestinnän mahdollistamiseksi. Yritys käyttää ulkoisen palveluntarjoajan luomaa domain-sertifikaattia. Domain-sertifikaatti suojaa yrityksen domainin sisällä tapahtuvan viestinnän.

Matkustaville työntekijöille on asetettu oma portti Helsingin palomuuriin, johon he ottavat VPN-yhteyden. Myös etäkonttorin työntekijät lukevat Helsingin Exchange- palvelimelta sähköpostinsa. Helsingin ja etäkonttoreiden välinen yhteys tapahtuu niin sanotulla site-to-site -VPN tunnelilla, joka toteutetaan IPSEC- tietoliikenneprotokollalla. Exchange- palvelimella on käytössä Outlook Autodiscovery toiminto, jolloin yhteys Outlookin ja Exchange- palvelimen välillä reititetään yritysverkon ulkopuolelta käyttämällä ulkoista sertifikaattia (SSL-Certificate) ja ohjaamalla toiminta Forefront Threat Management Gateway-tietoturvapalvelimen ylitse.



Kuva 1: Yrityksen sähköpostijärjestelmä

Ongelmaksi muodostuu yrityksen etäkonttori Kiinassa. Yhteys Kiinan konttorilta Helsingin sähköpostipalvelimelle on liian hidas tehokkaaseen ja hyödylliseen sähköpostiviestintään. Tämän vuoksi asiakasohjelman sijaan, Kiinan konttorin sähköpostit ohjataan Exchange-palvelimelta lokaalioperaattorien sähköpostilaatikkoon. Kiinan konttorin palomuuri ohjaa kaiken muun kuin Helsinkiin menevän liikenteen suoraan Kiinan operaattorin verkkoon. Sähköpostin ohjautuessa lokaalisähköpostilaatikkoon, viesti poistuu domainista, jolloin myös domain-sertifikaatin kryptaus purkautuu. Sähköposti siirtyy nyt suojaamattomana internetin läpi ”vieraaseen” sähköpostilaatikkoon. Tämä muodostaa kriittisen tietoturvaongelman yrityksen sisäiseen viestintään.



Kuva 2: Sähköpostijärjestelmän ongelmakohta

1.4 Tavoite ja rajaus

Yrityksen yhteyshenkilön kanssa sovittiin kolme mahdollista ratkaisumenetelmää sähköpostiliikenteen parantamiseksi. Jokaisen ratkaisumenetelmän toimivuus tutkitaan teoreettisella tasolla, jonka jälkeen yksi näistä menetelmistä valitaan tarkempaan tutkintaan. Jokaisen ratkaisun hyvät ja huonot puolet punnitaan yhdessä, jonka perusteella paras ratkaisuvaihtoehto valitaan. Tavoitteena on saada turvallinen ja toimiva sähköpostiliikenne Kiinassa sijaitsevan etäkonttorin ja Helsingin pääkonttorin välille.

Ratkaisun on pystyttävä vaikuttamaan kahteen epäkohtaan. Sen on lisättävä nopeutta ja tehokkuutta Helsingin ja Kiinan konttorin väliseen sähköpostiliikenteeseen. Tämän lisäksi sen on myös pystyttävä ratkomaan olemassa oleva tietoturvariski tämän hetkisessä sähköpostiliikenteessä. Kohdeyritys asetti seuraavat kriteerit ratkaisun valintaan:

- Aikaisempi kokemus ratkaisuun.
  On suotavaa, että menetelmä on niin sanotusti Best practise- ratkaisu, joka on aikaisemmin ollut, tai on tälläkin hetkellä käytössä.

- Kustannustehokas ratkaisu.
  Resursseja tulee käyttää ratkaisun suunnitteluun ja toteuttamiseen vain se määrä, mitä yrityksellä on tarjota.

- Joustavuus.
  Ratkaisua on pystyttävä muokkaamaan mahdollisten muutoksien tapahtuessa.

- Hyödyllisyys tulevaisuudessa.
  Ratkaisun olisi soveliasta pystyä ratkaisemaan myöhemmin myös muita samankaltaisia ongelmia.

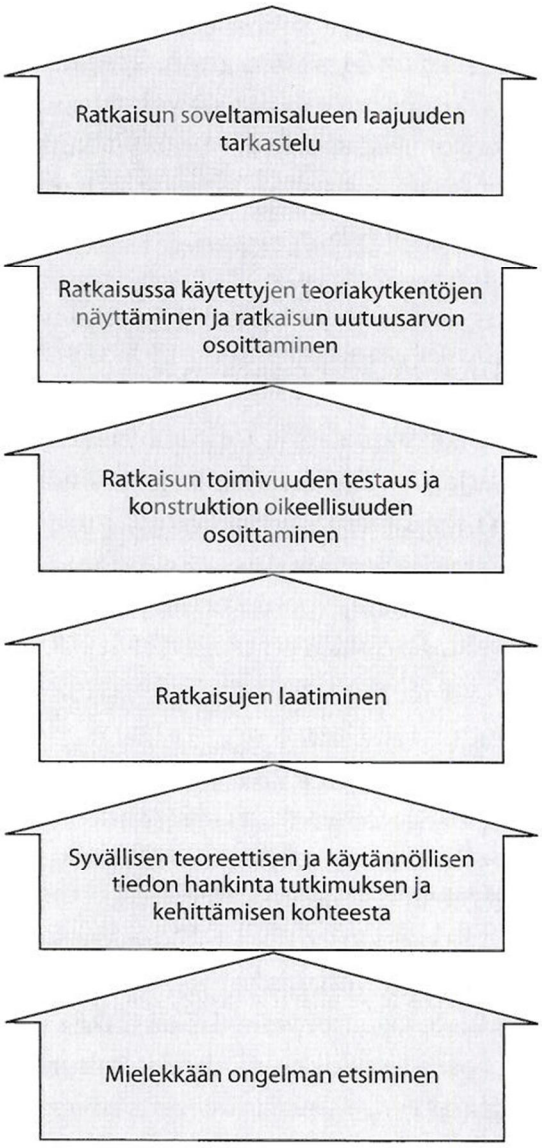
- Skaalautuvuus
  Onko ratkaisu yhteensopiva yrityksen muun ohjelmistoympäristön kanssa.

Näiden kriteereiden perusteella valittiin seuraavat menetelmät: Erillinen VPN-yhteys sähköpostiliikenteeseen, erillinen digitaalinen sertifikaatti etäkonttorin ja Helsingin konttorin väliseen sähköpostiliikenteeseen ja erillisen sähköpostijärjestelmän käyttöönotto etäkonttorille.

1.5 Tutkimusmenetelmä

Opinnäytetyössä käytettiin konstruktiivista tutkimusmenetelmää. Konstruktiivisessa tutkimuksessa pyritään luomaan jokin konkreettinen tuotos tutkimustiedon pohjalta. Konstruktiivisessa tutkimuksessa haetaan hyvin käytännönläheistä ongelmaratkaisua luomalla uusi rakenne jo olemassa olevan tilalle. Tähän tarvitaan paljon jo olemassa olevaa teoreettista tietoa ja uutta empiiristä tietoa (Ojasalo, Moilanen & Ritalahti 2009, 65).

Konstruktiivinen tutkimusmenetelmä oli paras vaihtoehto opinnäytetyöhön, koska kyseessä on tunnettu ongelma, johon on jo olemassa ratkaisu. Tehtäväksi jääkin ratkaisuvaihtoehtojen tutkiminen ja niistä toimivin vaihtoehto. Ojasalon, Moilasen ja Ritalahden (2009, 66) mukaan ”konstruktiivinen tutkimus soveltuu hyvin lähestymistavaksi kun tehtävänä on luoda konkreettinen tuotos, esimerkiksi uusi tuote, järjestelmä, malli tai suunnitelma”. He mainitsevat myös, että konstruktiivinen tutkimus pyrkii ratkaisemaan käytännön ongelman, jossa ratkaisun avaimia ovat kehittämisen yhteys aikaisempaan teoriaan, ongelman ja ratkaisun käytännön merkitys (2009, 66).



Kuva 3: Konstruktiivisen tutkimuksen prosessi (Ojasalo, Moilanen & Ritalahti 2009, 67)

Opinnäytetyössä keskitytään prosessipuun neljään ensimmäiseen kohtaan. Konstruktiivinen tutkimus sopii myös siltä osin kyseiseen työhön, koska tämän opinnäytetyön tarkoitus on tutkia parhaiten soveltuva ratkaisu ongelmaan, mutta ei ottaa ratkaisua käyttöön. Ojasalo, Moilanen & Ritalahti päättää kappaleen sanoihin: ”Ratkaisun toimivuutta voidaan käytännössä arvioida joskus myös myöhemmin. Tämän takia esimerkiksi konstruktiivisen tutkimuksen raporteista voi puuttua lähestymistavalle tyypillinen ratkaisun testaus erityisesti silloin, kun kyse on opinnäytetyöstä tai muusta työstä, joka on sidottu joltakin muulta osin muun kuin kohdeorganisaation aikatauluihin” (2009, 68).

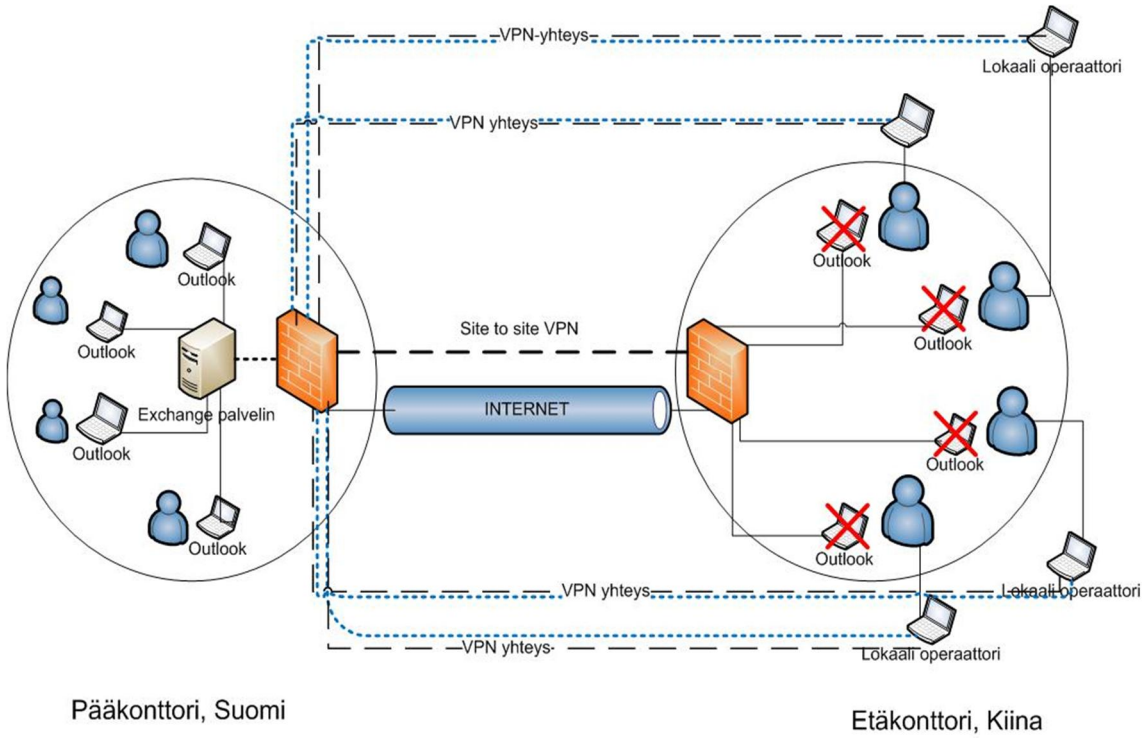
2 Tietoturvaratkaisut

Tämä kappale käsittelee mahdolliset tietoturvaratkaisut tutkimusongelmaan. Kappaleessa kuvataan yleisesti jokaisen ratkaisu käsitteenä ja sen toimivuus yleisesti, jonka jälkeen esitetään teoreettinen tomintamalli tutkimusongelmaan. Toimintamallit kuvataan sillä oletusarvolla, että ne ratkaisisivat ongelman. Kappaleen tarkoituksena on avata ratkaisut käsitteinä ja esittää hypoteesit ongelmanratkaisuun.

2.1 Erillinen VPN-yhteys sähköpostiliikenteeseen

VPN, eli Virtual Private Network, on virtuaalinen yksityisverkko, joka voidaan rakentaa julkisen verkon yli suojaamaan siirrettävää dataa. Perimutter ja Zarkower kuvailee VPN:ää seuraavasti: ”VPN on tietoliikenneverkko, joka on rakennettu yrityksen yksityiseen käyttöön jaetun julkisen infrastruktuurin välityksellä. Tämä määritelmä kattaa kaksi ensisijaista sovellusta: etäyhteydet ja eri toimipaikkojen väliset yhteydet” (2001, 10). VPN voidaan kuvastaa eräänlaisena putkena, jonka sisällä tietoliikenne tapahtuu. Putken päät ovat määritetty esimerkiksi yrityksen yksityisestä verkosta etäkonttorille tai työntekijälle, jolloin voidaan varmistaa että siirrettävä tieto pysyy vai niiden halussa ketkä ovat oikeutettuja siihen. (Tyson & Crawford 2012)

Virtual private networkia voitaisiin hyödyntää ongelmaan rakentamalla oma VPN väylä paikallisen operaattorin ja yrityksen domainin välille. Palomuuri toimisi tässä tapauksessa VPN-palvelimena, johon yhteys otettaisiin viestiä lähettäessä. Yhteys voitaisiin säilyttää koko ajan koneen ollessa päällä, jolloin yhteyttä ei tarvitsis erikseen joka kerta avata. Verkkoa hallinnoiva taho määrittäisi yhteydenottajalle oikeuden päästä kyseiseen verkkoon ja yhteydenottajan aitous varmistetaan antamalla käyttäjätunnus ja salasana.

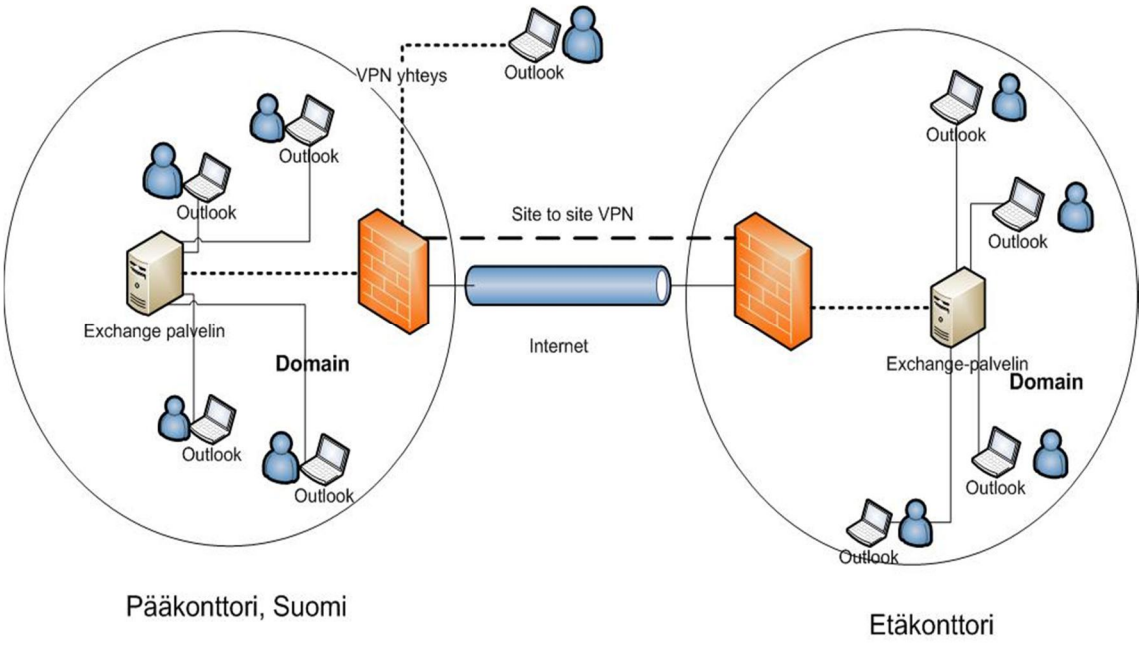


Kuva 4: Sähköpostiliikenteen salaus VPN-yhteydellä

2.2 Exchange-palvelimen asennus Kiinan etäkonttoriin

Microsoft Exchange- sähköpostipalvelin Microsoftin kehittämä viestintäpalvelu, joka yhdistää sähköpostin, kalenteripalvelut, yhteystietokannan ja vastaajaratkaisut. Microsoft Exchange-palvelin toimii yhteistyössä Microsoft Outlook- asiakasohjelman kanssa. Exchange-palvelimelle luodaan yrityksen työntekijöiden sähköpostitilit, joihin otetaan yhteys asiakasohjelmalla.

Etäkonttoriin asennettaisiin toinen Exchange-palvelin, johon etäkonttorin Outlook-asiakasohjelmat ottaisivat yhteyden. Etäkonttorin työntekijöiden sähköpostitilit luotaisiin omaan sähköpostipalvelimeen Helsingin sähköpostipalvelimen sijaan. Etäkonttorin sähköpostipalvelin ottaisi tämän jälkeen yhteyden Helsingin konttorin palvelimeen ja keskustelu tapahtuisi reaaliaikaisesti. Palvelimien keskenäinen konfigurointi auttaisi viestiliikenteen nopeuteen huomattavasti. Kumpikin palvelin sijaitsisi yrityksen domainissa, jolloin yrityksen sisäinen domain-sertifikaatti pitäisi viestiliikenteen suojattuna. Sama käytäntö voitaisiin toteuttaa myös ostamalla samanlainen palvelu ulkoiselta tarjoajalta.

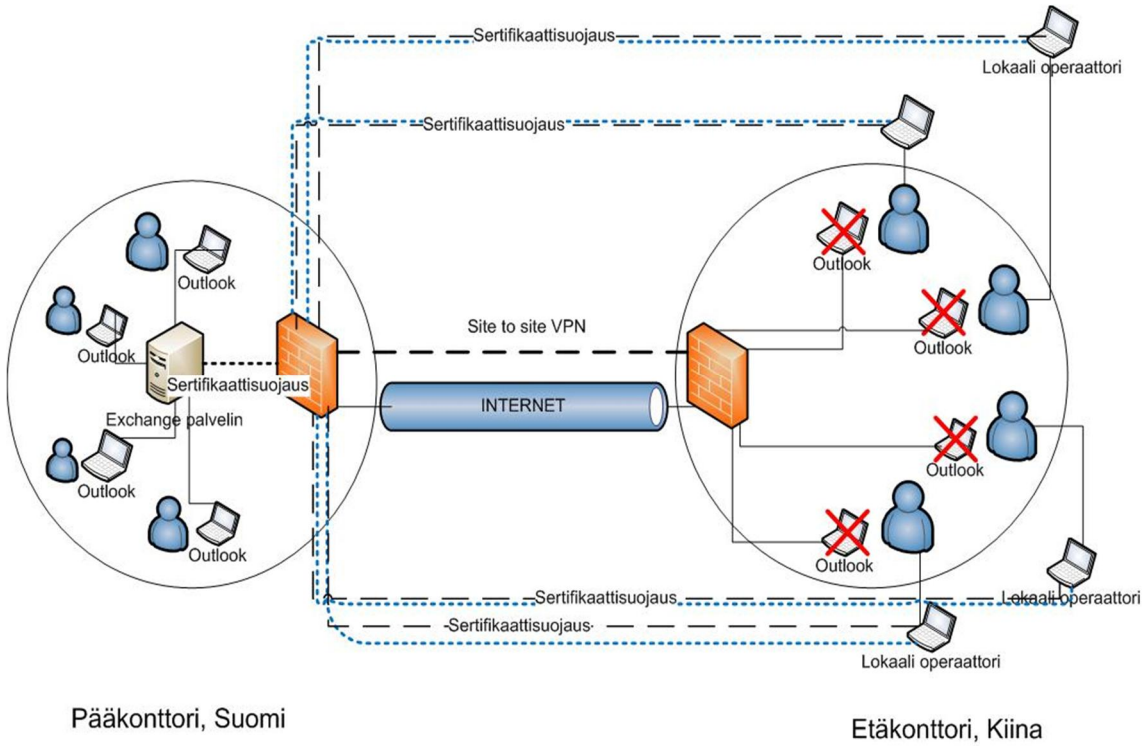


Kuva 5: Toisen Exchange-järjestelmän käyttöönotto

2.3 Digitaalinen sertifikaatti

Digitaalinen sertifikaatti, tai digital ID, on Internetiä varten suunniteltu elektroninen tunniste. Digitaalisen sertifikaatin tarkoituksena on vahvistaa sertifikaatin omistaja. Sertifikaatit myönnetään varmenneviranomaisen kautta, ja samalla tarkastetaan sertifikaatin omistajan aitous. Digital IDn teknologia perustuu julkisen avaimen kryptografiaan. Jokaisella taholla on kaksi avainta, julkinen avain ja salainen avain. Nämä kaksi avainta toimivat vain yhdessä. Tarkoituksena on yhdistää luotettavasti julkisen ja salaisen avaimen parit omistajien kesken. Tunnetuimpia palveluntarjoajia ovat mm. Verisign ja GoDaddy (Comodo 2012).

Digitaalinen sertifikaatti upotettaisiin sähköpostiin ennen sen lähettämistä. Sertifikaatin avaimet jaettaisiin Helsingin Exchange-palvelimelle ja etäkonttorin työntekijöille. Palvelin voitaisiin esimerkiksi konfiguroida käyttämään sertifikaattia, aina kun viesti on siirtymässä etäkonttoriin. VPN-yhteyden tavoin viestiliikenne olisi sertifikaatin avulla suojattua, ilman liikenteen hidastumista.



Kuva 6: Sähköpostiliikenteen suojaus sähköisellä sertifikaatilla

3 Ratkaisumenetelmän valitseminen

Tutkimuksen kohteeksi valittiin toisen Exchange-palvelun hyödyntäminen. Kriteereiden perustella tehty vertailu näiden vaihtoehtojen kesken osoitti Exchange-palvelun ylivoimaisuuden muihin verrattuna. Suurimman eron menetelmiin aiheutti skaalautuvuus ja tulevaisuuden hyödyntäminen. Lisäksi Exchange-palvelu oli ainoa menetelmistä, joka voisi lisätä tehokkuutta ja nopeutta oleellisesti sähköpostiliikenteeseen.

VPN- ratkaisumentelmä ratkaisisi tietoturvaongelman, mutta sen hyödyntäminen tulevaisuudessa jäisi lähes olemattomaksi. Uusilla työntekijöillä etäkonttorilla pitäisi olla käytössä saman kolmannen osapuolen tarjoama henkilökohtainen sähköposti, jotta VPN-ratkaisu olisi käyttökelpoinen. Mikäli käyttössä olisi joku muu lokaali sähköposti, jouduttaisiin tekemään kokonaan uusi VPN sopimus uuden palveluntarjoajan kanssa. Mitään varmuutta ei ole, voidaanko sopimusta lokaalioperaattorin kanssa edes tehdä. Ratkaisun budjetointiakin on vaikea pohtia tässä tapauksessa, koska kyseessä on ”tuntematon” lokaalioperaattori eri mantereella.

Digitaalisen sertifikaatin käyttöönotto sisälsi samoja ongelmia. Sekin ratkaisisi tietoturvaongelman, mutta VPN-ratkaisun tavoin sen hyödyllisyys tulevaisuudessa jäisi vähäiseksi. Uusi erillinen sertifikaatti pitäisi räätälöidä lokaalioperaattorin ja pääkonttorin väliseen sähköpostiliikenteeseen, jolloin sen käyttö vastaavanlaiseen ongelmaan eri

ympäristöissä olisi kyseenalaista yhteensopivuuksien takia. Lisäksi varmistettavaksi jäisi domain-sertifikaatin ja erillisen sertifikaatin yhteiskäyttö.

Lähtökohtaisesti yritys haluaisi sähköpostijärjestelmän yhtenäistämistä konttorista riippumatta, jolloin kaikki ottaisivat käyttöön Outlook-asiakasohjelmat. Suurin syy tähän on vieraan sähköpostin hallitsemattomuus. Koska Kiinan työntekijöiden käyttämät vieraat sähköpostilaatikot eivät ole yrityksen omistuksessa, sähköpostilaatikon sisältö ei ole hallittavissa. VPN ja digitaalinen sertifikaatti eivät soveltuneet tähän skenaarioon. Erillisen Exchange-järjestelmän hyödyntäminen ongelmaan sen sijaan täyttää aikaisemmin mainittujen kriteereiden lisäksi myös yllä olevan ongelman.

Exchange-järjestelmän käyttöönotto voidaan ratkaista monella eri tavalla. Tutkittavaksi otetaan kolme mahdollista ratkaisumenetelmää, joista jokaisen ratkaisun toiminta käydään läpi teoriassa ja sen jälkeen kuvataan teoreettinen käyttöönotto. Käyttöönoton hyvät ja huonot puolet punnitaan ja niitä vertaillaan keskenään.

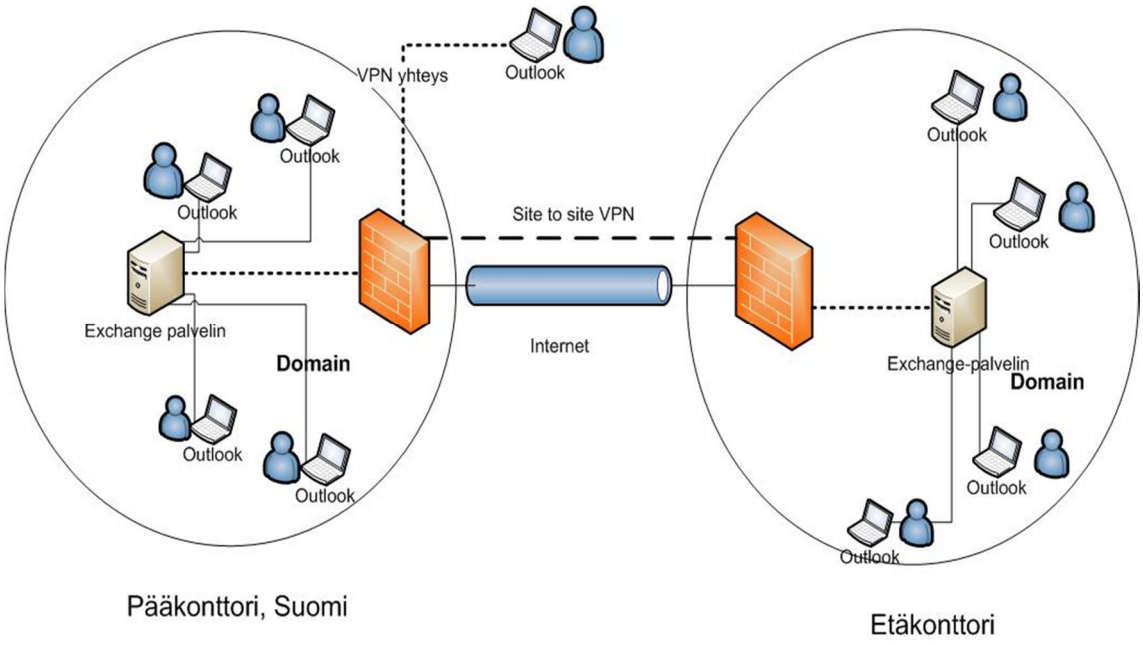
Vertailun perusteella rakennetaan yhteen ratkaisumenetelmään perustuva testiympäristö. Testiympäristöllä on tarkoitus kokeilla käyttöönottoa käytännössä ja osoittaa miten kyseinen menetelmä toimisi ratkaisuna. Tarkoitus on osoittaa yritykselle menetelmän vaikutus ongelmaan, jonka perusteella yritys voi hyödyntää myöhemmin ratkaisua käytännössä.

3.1 Ratkaisuvaihtoehdot

Kolme eri ratkaisumenetelmää valittiin tutkittavaksi: Fyysisen Exchange-lokaalipalvelimen rakentaminen etäkonttorille, Microsoft Office 365- pilvipalvelun käyttäminen ja Exchange-palvelun ostaminen kolmannelta osapuolelta.

3.1.1 Exchange- lokaalipalvelin

Exchange- lokaalipalvelin ostettaisiin ja asennettaisiin ensin Suomessa, jolloin myös tehtäisiin tarvittavat konfiguraatiot kahden sähköpostipalvelimen välille. Etäkonttorin sähköpostilaatikot siirrettäisiin uudelle palvelimelle ja asiakasohjelmat konfiguroitaisiin ottamaan yhteys uudelle palvelimelle. Uusi Sähköpostipalvelin sijoitettaisiin etäkonttorin tiloihin Kiinaan. Site to site VPN ehostaisi liikenteen salausta pitämällä liikenteen omassa verkossa, kun taas domainsertifikaatti suojaisi sähköpostit palvelimien välillä. Staattinen retitys taas nopeuttaisi liikennettä.

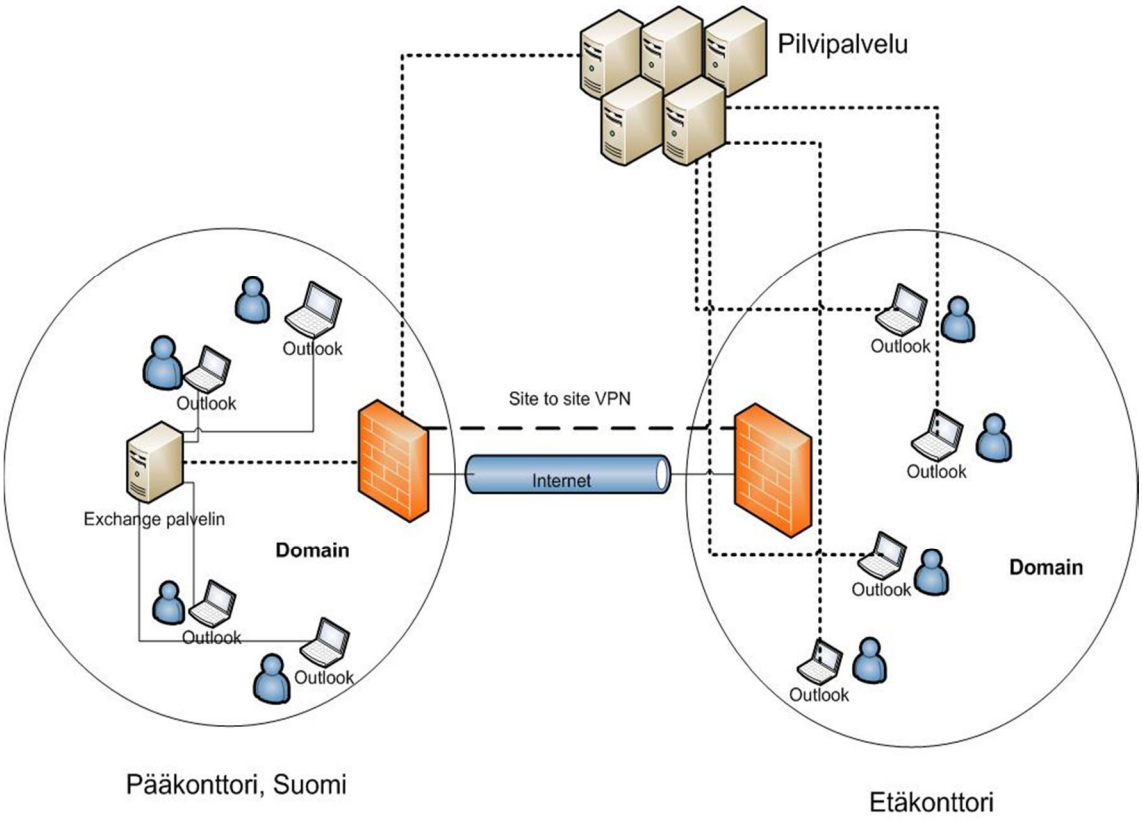


Kuva 7: Toisen lokaalipalvelimen käyttöönotto

3.1.2 Microsoft Office 365

Microsoft Office 365 on Microsoftin tarjoama pilvipalvelu. Se tarjoaa monet eri Microsoftin työkalut, joko erikseen, tai samassa paketissa pilvitekniikalla. Yksi näistä työkaluista on Exchange Online. Exchange Online toimii Microsoft Exchange-palvelimen tavoin sähköpostipalvelimena yritykselle, mutta fyysisen palvelimen sijaan se sijaitsee pilvessä. Exchange Online on yhteensopiva Microsoftin asiakasohjelmien kanssa, joten se toimisi yhdessä yrityksen Outlook- ohjelmien, sekä sähköpostipalvelimen kanssa. (Microsoft 2012.)

Palvelun ostamisen jälkeen Office 365 liitettäisiin yrityksen domainiin. Tämän jälkeen etäkonttorin sähköpostilaatikot siirrettäisiin yrityksen sähköpostipalvelimelta Exchange Online- pilvipalvelimeen. Etäkonttorin Outlook- asiakasohjelmat konfiguroitaisiin ottamaan yhteys pilvipalveluun tämän jälkeen. Viestiliikenne reititettäisiin Exchange-sähköpostipalvelimen ja pilvipalvelimen välille, jolloin yrityksen domainsertifikaatin tarjoama suojaus säilyisi koko viestiliikenteen ajan. Koska palvelimien välille konfiguroitaisiin kiinteä reitti sähköpostiliikenteelle, nopeutuisi liikenne myös huomattavasti olemassa olevaan ratkaisuun nähden.

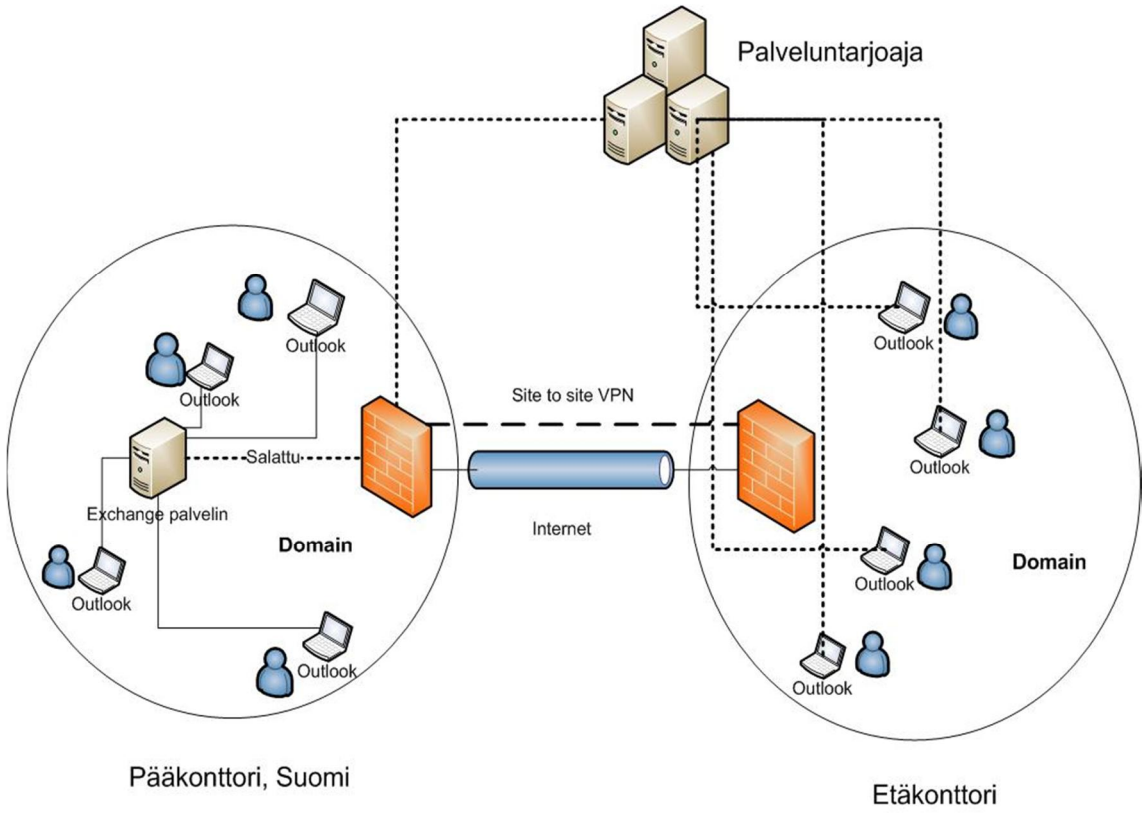


Kuva 8: Microsoft Office 365 – pilvipalvelu

3.1.3 Kolmannen osapuolen Exchange- palvelu

Exchange-palvelun käyttöönotto kolmannelta osapuolelta tapahtuisi samalla periaatteella kuin pilvipalvelukin. Erona kuitenki olisi se, että Microsoftin sijaan kyseessä olisi niin sanottu välikäsi, palveluntarjoaja, joka tarjoaisi Microsoftin palveluita.

Tässä tapauksessa Exchange-sähköpostipalvelin sijaitsisi fyysiseltä olemukseltaan palveluntarjoajan isännöimässä palvelinsalissa, johon asennettaisiin erillinen palvelin etäkonttoria varten. Yrityksen etäkonttorin työntekijöiden sähköpostilaatikot siirrettäisiin yrityksen sähköpostipalvelimelta palveluntarjoajan palvelimelle, jonka jälkeen asiakasohjelmat konfiguroitaisiin ottamaan yhteyttä kyseiselle palvelimelle omiin sähköpostilaatikoihin. Reititys konfiguroitaisiin palvelimien välille, kuten pilvipalvelussakin. Näin nopeuteen voitaisiin vaikuttaa huomattavasti staattisen reitityksen takia. Kummatkin palvelimet kuuluisivat yrityksen domainiin, joka mahdollistaisi domainsertifikaatin toimivuuden.



Kuva 9: Kolmannen osapuolen tarjoama Exchange-palvelu

3.2 Ratkaisuun vaikuttavat tekijät

Menetelmää valittaessa joudutaan pohtimaan uusia tekijöitä, jotka vaikuttavat lopulliseen valintaan. Koska aikaisemmin mainitut kriteerit täyttyvät tutkittavissa menetelmissä, joudutaan kriteereitä nostamaan korkeammalle. Menetelmän valintaan vaikuttaa suuresti sen pitkäkestoisuus, kustannustehokkuus pitkällä aikavälillä, yhteensopivuus ja hyödynnettävyys yrityksen muun työympäristön kanssa.

3.2.1 Lokaalipalvelimen ja pilvipalvelun vertailu

Pilvipalvelu ja lokaalipalvelin toimivat yleisiltä ominaisuuksiltaan lähes identtisesti. Siksi joudutaan pohtimaan, halutaanko ratkaisu itselle hoidettavaksi vai ulkoistetaanko se jollekkin muulle. Koska ratkaisu ongelmiin löytyy kummastakin vaihtoehdosta, joudutaan kartoittamaan kummankin vaihtoehdon hyödyllisyys pidemmällä aikavälillä.
Suurimmat erot näiden kahden välillä ovat työkuormitus ja kustannukset. Lokaalipalvelin tulee maksamaan yritykselle sen hankinnasta eteenpäin aina konfiguroinnin kautta sijoitukseen saakka. Pilvipalvelut tarjoavat kiinteää kuukausimaksua vastaan samat palvelut ilman erillisiä lisäkustannuksia.

Huoltotoimenpiteet ovat elintärkeitä palvelun toimivuuden ja luotettavuuden kannalta. Huoltotoimenpiteisiin kuuluvat palvelun päivitys, ylläpito ja fyysisen ”raudan” huolto. Lokaalipalvelimen käyttöönotossa nämä toimenpiteet jäävät yrityksen IT-osaston vastuulle. Kiinan konttorilla ei ole työntekijää, joka olisi pätevä hoitamaan näitä tehtäviä, joten ne jouduttaisiin tekemään etätyönä Helsingin pääkonttorilta. Nämä tehtävät kuormittavat IT-osastoa huomattavasti. Pilvipalveluiden tarjoajat sen sijaan itse lupautuvat hoitamaan nämä työt, jolloin ainoastaan itse yrityksen vaatimat toimenpiteet jäisivät IT-osaston vastuulle. Pilvipalvelut myös lupaavat sopimuksessaan 99.9 prosentin varmuuden palvelimien toimivuudesta ja päällä olemisesta (SLA) (Microsoft 2012 & Sherweb).

Palvelimen sijaintia joudutaan miettimään kun puhutaan arkaluontoisesta materiaalista. Lokaalipalvelin olisi yrityksen hallussa myös fyysisesti verkkohallinnan lisäksi. Näin kenelläkään ulkopuolisella ei ole teoriassa mahdollisuutta päästä käsiksi palvelimeen fyysisesti, eikä verkon yli. Asia ei kuitenkaan ole niin yksinkertainen. Tietoturvan näkökulmasta katsottuna pelkästään yrityksen tiloissa sijaitseva palvelin ei ole tietoturvallinen. Palvelimelle pitäisi miettiä sijainti, jossa se ei ole kaikkien näkyvillä, sekä sen pitäisi olla turvassa niin sanotuilta luonnon tietoturvauhilta, kuten tulipalolta sekä vesivahingoilta. Lisäksi palvelimen pitäisi olla jatkuvan jäähdytyksen kohteena ylikuumentumisen ehkäisemiseksi.

Vikatilanteiden sattuessa pitää olla mahdollista saada tukea korjauksiin. Lokaalipalveliratkaisussa niin sanotut huoltotoimenpiteet jäävät yrityksen IT-osaston vastuulle. Fyysisen vian sattuessa reaktioaika kasvaa huomattavasti, koska jonkun on mentävä paikan päälle hoitamaan vika. Parhain mahdollinen tilanne olisi palvelun ympäri vuorokautinen päivystys. Tähän yrityksen resurssit eivät kuitenkaan riitä.

Pilvipalvelut tarjoavat erilaisia tuki- ja huoltopalveluita riippuen sopimuksesta. Yleisesti voidaan ajatella, että jokainen ulkoistettu palvelu tarjoaa yleisen tuen ja reaktioajan mahdollisille vioille.

3.2.2 Pilvipalveluiden vertailu

Vertailtaviksi kohteiksi valittiin Microsoft Office 365 palvelu, sekä yksi kansainvälinen palveluntarjoaja nimeltä Sherweb. Kummankin tarjonnat ovat päällisin puolin samanalaiset lähes identtiseen hintaan. Kuten alla olevasta taulukosta näkyy, tärkeät, oletusarvoiset palvelut ovat kummallakin palveluntarjoajalla lähes identtiset lähes samaan hintaan.

Palvelut		Office 365 Exchange Online	Sherweb Professional
Outlook integrointi		X	?
Postilaatikon koko		25 Gb	25 Gb
CSF		X	X
Kalenterin jako		X	X
AD synkronointi		X	X
Tuki		X	X
Hosted Lync		-	IM/tilapäivitys
Hosted Sharepoint		-	1 Gb

Taulukko 1: Palveluiden vertailu (Microsoft 2012 & Sherweb)

Vertailtavaksi jäävät enää pienemmät yksityiskohdat eri palveluntarjoajien välillä. Esimerkiksi Sherweb tarjoaa paketeissaan lisäpalveluita, kuten Microsoft Sharepoint Online-dokumentinhallinta-alustaa ja Lync Online- pikaviestintäpalvelua (Sherweb). Yrityksellä on kuitenkin jo käytössä Lync-, sekä Sharepoint- palvelut, joten nämä lisäominaisuudet jäisivät ylimääräisiksi. Microsoft Office 365 tarjoaa pelkästään Exchange- palvelua, jolloin hinta putoaa alhaisemmaksi, eikä ylimääräisiä palveluita tule käyttöön. Microsoftin avoimuus palveluiden fyysisestä sijainnista ja muista selvityksistä kuten esimerkiksi safeharbour-käytänteistä, katsotaan vahvuudeksi palvelua valittaessa. Epäselväksi jää myös lokaalipalvelimen ja pilvipalvelun yhteistyökyky palveluntarjoajan osalta. Testattavaksi palveluksi valittiin näiden asioiden myötä Microsoft Office 365.

3.3 Microsoft Office 365- palvelun demoympäristön rakentaminen ja testikäyttö

Demoympäristön rakentaminen alkoi Microsoft Office 365- trial paketin hankinnalla. Kuukauden ajaksi tarkoitettu testiversio otettiin käyttöön luomalla avainhenkilöille tilapäiset sähköpostiosoitteet pilvipalveluun. Avainhenkilöille luotiin myös administraattorioikeudet palveluiden kartoittamista varten. Seuraavaksi Kiinan etäkonttorin työntekijöille luotiin tavalliset käyttäjäkohtaiset sähköpostiosoitteet. Osoitteet luotiin samalla periaatteella kuin jo käytössä olevat yrityksen sähköpostiosoitteet. Testikäyttöä varten ei työntekijöille asetettu erityisoikeuksia, koska tarkoitus oli vain saada palautetta kyseisen postipalvelun toiminnasta. Käyttäjien perusoikeuksiin kuului vain henkilökohtaisten tietojen päivittäminen ja postin vastaanottaminen ja lähettäminen. Kontrolliryhmäksi valittiin Japanin konttori, jonka työntekijöille luotiin myös samalla periaatteella tilapäiset sähköpostiosoitteet.

Demoympäristön testikäyttöön osallistuville työntekijöille lähetettiin seuraava sähköposti:

"Hello,

We are testing new Microsoft Office 365 cloud service and we would like you to participate in this project. We have created a temporary email boxes for you and we would like to get your input (does it work, is it fast/efficient etc.) on this matter. All mail traffic to your XXXX email account will also be forwarded to your new Exchange online accounts. If you could try the new Exchange online service and compare it to your XXXX email account for the next week or so and then send us feedback at ville.saarinen@xxxx.onmicrosoft.com. It would be much appreciated.

I will send email addresses and temporary passwords to each of you via email. If you have any questions, contact via email: ville.saarinen@xxxx.onmicrosoft.com or Lync: Ville Saarinen. I'll also attach instructions so that you can add the Exchange online email account to your Outlook client.
Thank you very much in advance!

Br,
Ville Saarinen
IT Support
ville.saarinen@xxxx.fi"

Yrityksen omiin sähköpostiosoitteisiin kulkeva sähköpostiliikenne ohjattiin myös pilvipalveluun ja työntekijöitä pyydettiin käyttämään testipalvelua seuraavan kahden viikon ajan. Jokaiselle työntekijälle lähetettiin henkilökohtaisessa sähköpostissa käyttäjätunnus/sähköpostiosoite sekä tilapäinen salasana. Liitteenä oli myös ohje, jonka avulla Exchange Online- sähköpostitili saatiin lisättyä henkilökohtaiseen Outlook- asiakasohjelmaan (kts. liite 1).

Testin tarkoituksena oli saada palautetta pilvipalvelun sähköpostitilin käytöstä ja nopeudesta. Nopeutta seurattiin lisäämällä sähköpostitili outlook-asiakasohjelmaan, jotta voitaisiin nähdä lokaalipalvelimen ja pilvipalvelun latenssierot. Tavoitteena oli, että sähköpostiviestin uudelleenohjaus yrityksen sähköpostista pilvipalveluun saapuisi nopeammin pilvipalvelun sähköpostiin, jolloin voitaisiin olettaa, että pilvipalvelun käyttöönotto korjaisi Kiinan konttorin hitaan ja tehottoman yhteyden. Kontrolliryhmältä haluttiin saada palautetta samasta aiheesta, jotta nähtäisiin vastaavasti, vaikuttaisiko se mahdollisesti sähköpostiliikenteen nopeuteen negatiivisella tavalla. Näin saataisiin kahden Aasian konttorin palautteet, joita voitaisiin vertailla ja tehdä johtopäätökset pilvipalvelun toimivuudesta.

Osallistujille annettiin noin kolme viikkoa aikaa testikäyttöön, jonka jälkeen heiltä pyydettiin palautetta seuraavalla sähköpostilla:
"Hello everyone,

First of all, thanks to all of you, who have already given us feedback about the Microsoft Office 365 Exchange Online service.

At the moment we are considering on taking this service into use in some of our remote offices, which is why it is important for us to get your feedback about this service. The decision will be made based on your feedback. If we decide to take this service to use, it will be migrated to our XXXX.fi domain, which means that your email address will be firstname.lastname@XXXX.fi when sending and receiving emails.

The reasons, why we are considering this service, are;

1. *To improve the efficiency of internal email traffic.*
2. *To improve the security of internal email traffic.*
3. *To unify the company brand in email traffic.*

All kinds of feedback are still very much appreciated.

If you have any questions regarding this matter, please contact ville.saarinen@XXXX.fi or XXX.XXXXXX@XXXX.fi

Thank you very much in advance!

Br,

Ville Saarinen
IT Support
ville.saarinen@xxxx.fi"

Yrityksen toiminimen liittämistä pilvipalveluun testattiin myös. Toiminimen liittäminen onnistui ilman ongelmia ja liittäminen dokumentoitiin kuvakaappauksilla (kts. liite 2).

4 Tulokset ja johtopäätökset

Opinnäytetyössä tutkittiin yrityksen sähköpostiliikenteen tietoturva-aukon paikkaamista eri menetelmillä. Kolme erilaista vaihtoehtoa tutkittiin teoriassa ja näistä yksi menetelmä valittiin tarkempaan tutkimukseen. Menetelmän toteutus kuvattiin kolmella eri tavalla ja näistä parhaiten soveltuva vaihtoehto esitettiin toteutettavaksi yritykselle. Testiympäristön rakentaminen ja koekäyttö antoi positiivisen vaikutelman ratkaisun toimivuudesta.

Testiympäristön osallistujien palautetta ei saatu niin paljoa kuin toivottiin. Vain pieni osa osallistujista vastasi kyselyihin rakentavalla palautteella. Palaute oli kuitenkin suurimmaksi osin myönteistä. Kiinan työntekijöiden palaute oli positiivisesti yllättävää. Tulosten mukaan pilvipalvelun käyttö oli huomattavasti nopeampaa ja tehokkaampaa kuin yrityksen oman sähköpostipalvelun.

Suomessa tehdyt testit eivät oletetusti näyttäneet voimakasta eroa palveluiden välillä. Viestit saapuivat kumpaankin postilaatikkoon lähes samaan aikaan, jolloin pilvipalvelu ei nopeuttanut liikennettä mutta se ei myöskään hidastanut sitä.

Japanin kontrolliryhmän palaute oli samaa luokkaa kuin Suomenkin. Heidän sähköpostiliikenne ei tehostunut dramaattisesti, mutta se ei myöskään hidastunut. Tästä voidaan päätellä, että pilvipalvelun käyttöönotto myöhemmässä vaiheessa muissa etäkonttoreissa ei pitäisi hidastaa liikennettä tehottomammaksi, kuin mitä se tällä hetkellä on.

Palautetta ei voida olettaa luotettavaksi, koska suurin osa osallistujista ei vastannut palautekyselyyn. Testaus kuitenkin antoi referenssiä siihen, miten palvelu teoriassa toimisi, jos se otettaisiin käyttöön.

Koska vain yhtä käyttöönottomenetelmää testattiin, on mahdotonta sanoa oliko kyseinen menetelmä paras ratkaisu. Voidaan vain spekuloida muiden vaihtoehtojen toiminnallisuutta. Kyseinen menetelmä kuitenkin antoi hyvää referenssiä toiminnallisuudestaan. Ratkaisu olisi varmasti löytynyt jokaisesta menetelmästä, mutta kokeilun ja tiedon perusteella Microsoftin pilvipalvelu oli ylitse muiden.

Teknisen toteutuksen jälkeen saattaa edessä olla toisenlainen haaste. Muutokset, vaikka kuinka pienet, voivat aiheuttaa suurtakin ihmetystä ja joskus jopa närkästystä työntekijöissä. Työntekijöiden on ehkä vaikea ymmärtää miksi tämäntapaisia muutoksia tehdään, jos he ovat jo tottuneet edellisiin toimintatapoihin. Siksi tilanne tulisi olla selitettävissä myös heille, jotka eivät ole tietoisia syvemmästä tietoturvasta, tai eivät ymmärrä potentiaalisia uhkia

nykytilanteessa. Vaikka kyseessä on vakava asia, johon tottumukset eivät vaikuta, työntekijöitä voisi siltikin valaista kyseisen tilanteen toimettomuudesta ja samalla selittää miksi uudistus on tehty. Näin työntekijöiden asenteeseen pystyttäisiin mahdollisesti vaikuttamaan positiivisesti ja he ottaisivat uudistuksen vastaan myönteisemmin.

4.1 Kehittämisehdotus

Vertailun ja tulosten perusteella suosittelen yritystä hyödyntämään Microsoft Office 365- pilvipalvelua. Office 365 Exchange Online- palvelupaketti soveltuisi parhaiten yrityksen tarpeisiin ja vaatimuksiin. Exchange Online- palvelupaketti tarjoaa pelkästään pilvipohjaisen sähköpostipalvelun ja tarvittavat lisäominaisuudet sujuvaan sähköpostikäyttöön.

Exchange Online- palvelupaketti mahdollistaa yrityksen lokaalisähköpostipalvelimen ja pilvipalvelun hybridikäytön, jolloin nämä kaksi palvelua keskustelevat keskenään parantaen sähköpostiliikenteen eheyttä ja tehokkuutta. Kiinan etäkonttoreiden sähköpostitilit voidaan siirtää yrityksen toimesta omalla aikataululla pilvipalveluun, kuitenkaan aiheuttamatta suurta tietoliikennekatkosta. Sähköpostinimien muoto pysyy samana, eikä migraatio vaadi loppukäyttäjältä muita toimenpiteitä kuin tilin muuttaminen outlook- asiakasohjelmaan. Toiminimen liittämisen ansiosta migraatio ei myöskään vaaranna tietoturvaa sähköpostiliikenteessä, vaikka tilit siirtyvätkin pois fyysiseltä palvelimelta pilveen.

Exchange Online- palvelupaketin käyttöönoton jälkeen palvelun käyttöä voidaan ehostaa Microsoftin Active Directory Federation Services (ADFS)- palvelintyökalun käyttöönotolla. ADFS- työkalu mahdollistaisin Microsoft Office 365- palvelun Single sign-on (SSO)- kirjautumisen. Single sign-on- kirjautuminen tehostaisi päivittäistä työskentelyä, vähentämällä ylimääräisten kirjautumisten määrää.

Exchange Online- palvelupaketti tarjoaa tulevaisuutta ajatellen varteenotettavan vaihtoehdon. Halutessaan yritys voi siirtyä, joko kerralla tai pikkuhiljaa, esimerkiksi konttori kerrallaan kokonaan pilveen. Tätä voidaan harkita esimerkiksi lokaalipalvelimen käyttöajan lähestyessä loppuaan. Näin päästäisiin eroon fyysisestä palvelimesta, ja sen aiheuttamista ylimääräisistä kustannuksista. Tämä säästäisi tulevaisuudessa paljon resursseja ja rahanmenoa yritykselle.

5 Yhteenveto ja loppuarviointi

Sähköpostin käyttö on nykyään arkipäivää niin siviilissä, kuin työelämässäkin. Sen helppokäyttöisyys ja houkuttelee ihmisiä hyödyntämään yhä enemmän ja enemmän. Työpohjaisen sähköpostiliikenteen kulmakivi on tehokkuuden lisäksi myös turvallisuus. Se, kumpi näistä kriteereistä, tehokkuus vai turvallisuus, on tärkeämpi, jää yrityksen päätettäväksi.

Nykypäivänä tietoturvaongelmiin on tarjolla lukuisia eri ratkaisuja. Siksi pelkästään ongelmanratkominen ei enää nykyään riitä. Monimutkaiset verkkorakenteet, eri alustojen käyttö yhteisessä työympäristössä, sekä yleinen osaaminen ja tietoisuus voi tehdä hyvästä ratkaisusta toiselle pelkästään suuremman ongelman. Tämän vuoksi ongelman lisäksi joudutaan myös pureutumaan syvemmin omiin osa-alueisiin, jotta voidaan tarkastella sopivaa ratkaisua juuri itselle.

Pilvipalvelut ovat tekemässä omaa paikkaansa tulevaisuuden verkkopalveluissa. Yhä useampi palveluntarjonta kohdistuu lokaalipalvelimien sijaan pilviteknologiaan. Pilvipalveluiden helppokäyttöisyys ja vaivattomuus tekevät niistä erittäin houkuttelevia yrityksille. Tästä hyvänä esimerkkinä löytyvät Microsoftin tarjoamat verkkopalvelut. Paljon helpompaa ja käytännöllisempää on ulkoistaa palvelu ammattilaisille ja itse suorittaa vain suoraan omaan liiketoimintaan liittyvät asiat.

Uskon että työstä on hyötyä yritykselle pidemmän aikavälin suunnitelmissa. Vaikka tietoturvaongelma onkin akuutti tapaus, ratkaisu itsessään tulee olemaan toimiva myös tulevaisuudessa, mikäli sitä ei haluta vielä ottaa käyttöön. Lisäksi se antaa referenssiä pilvipalveluille yleisesti ja osoittaa niiden hyvät ja huonot puolet. Näitä voidaan soveltaa myöhemmin erilaisiin kehitystilanteisiin, missä vaihtoehtona on siirtyä pilvipalvelun hyödyntämiseen.

Itselleni työ on avannut uusia näkemyksiä nykypäivän liiketoiminnasta, viestinnästä ja palveluntarjonnasta. Monet asiat, jotka ovat olleet tuttuja vain teoriassa, ovat työn myötä selkeytyneet myös käytännössä. Sähköpostiliikenne ja sen toiminnallisuus on avautunut minulle uudella tavalla. Testiympäristön rakentaminen oli erittäinen opettavainen projekti. Uskon että työ tulee olemaan myös minulle hyödyllinen tulevaisuudessa työelämässä.

Lähteet

Kirjalliset lähteet

Haasio, A. & Rauhala, T. 2002. Tehokkaammin sähköpostilla. Helsinki: Kirjastopalvelu.

Perimutter, B & Zarkower, J. 2001. Virtuaaliset yksityisverkot. Suomentaja Kokkonen, T. Helsinki: Edita.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. WSOYpro.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki Nordprint Ab.

Järvinen, P. 2002. Tietoturva & yksityisyys. 2. painos. Jyväskylä: Docendo Finland.

Nader, Johar C. 1998. Prentice Hall's illustrated dictionary of computing. 3. painos. A division of Simon & Schuster.

Sähköiset lähteet

Crawford, S. & Tyson, J. 2012. How VPNs work. Viitattu 11.11.2012. http://www.howstuffworks.com/vpn.htm

Microsoft. 2012. What is Office 365. Viitattu 05.12.2012. http://www.microsoft.com/en-us/office365/what-is-office365.aspx

Microsoft. 2013. Definition of a Security Vulnerability. Viitattu 13.01.2013. http://technet.microsoft.com/en-us/library/cc751383.aspx

Crawford, S. & Tyson, J. 2012. How VPNs work. Viitattu 11.11.2012. http://computer.howstuffworks.com/vpn4.htm

Fulton, Scott M. 2012. New Open Group Cloud Standard Introduces "XaaS" - Something as a Service. Viitattu 18.11.2012. http://readwrite.com/2012/01/19/new-open-group-cloud-standard

Microsoft. 2012. Description of the Secure Sockets Layer (SSL) Handshake. Viitattu 18.11.2012. http://support.microsoft.com/kb/257591

Friedl, Steve. Illustrated guide to IPsec. Viitattu 14.01.2013. http://www.unixwiz.net/techtips/iguide-ipsec.html

Wikipedia. 2013. Palvelutasosopimus. Viitattu 16.01.2013. http://fi.wikipedia.org/wiki/Palvelutasosopimus

Microsoft. 2013. Microsoft Office 365. Viitattu 10.01.2013. http://www.microsoft.com/en-us/office365/all-plans.aspx#plans

Sherweb. Compare SherWeb's Hosted Exchange 2010 Plans. Viitattu 10.01.2013. http://www.sherweb.com/en-eu/hosted-exchange/exchange-migration

Comodo. 2012. Digital ID. Viitattu 10.10.2012. http://www.instantssl.com/code-signing/code-signing-technical.html

Sherweb. Compare SherWeb's Hosted Exchange 2010 Plans. Viitattu 10.01.2013. http://www.sherweb.com/en-eu/hosted-exchange/compare-plans

Kuvat ja kuviot

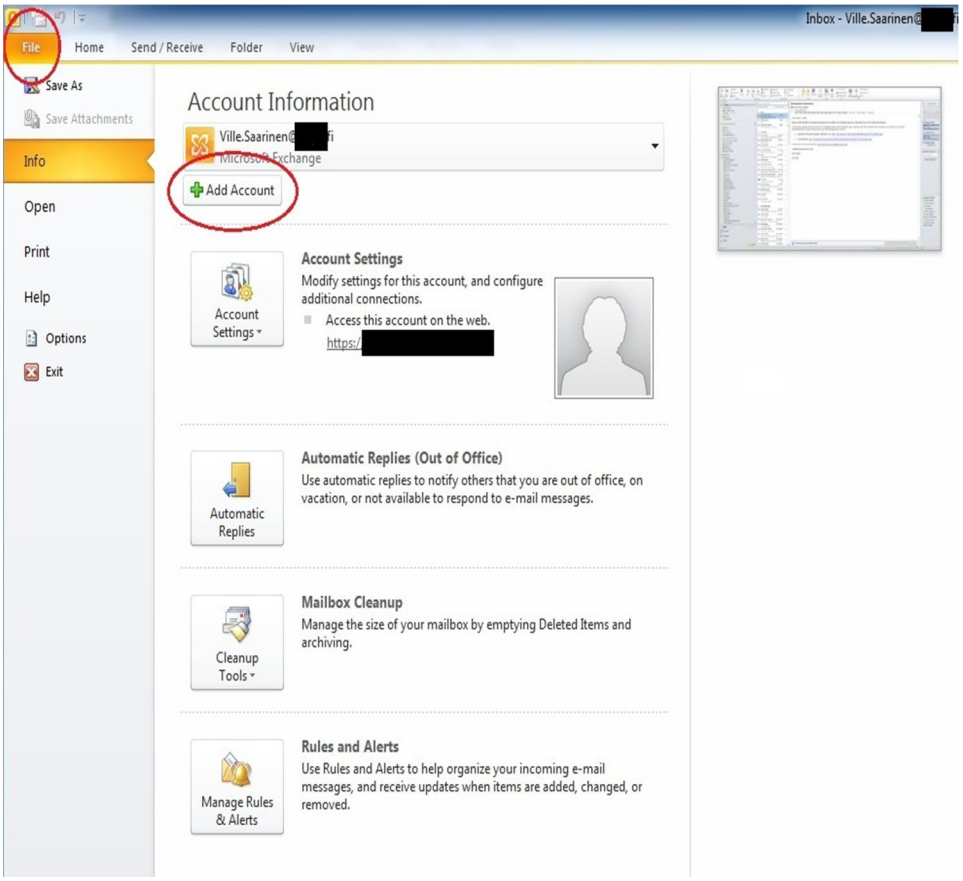
Taulukot

Liitteet

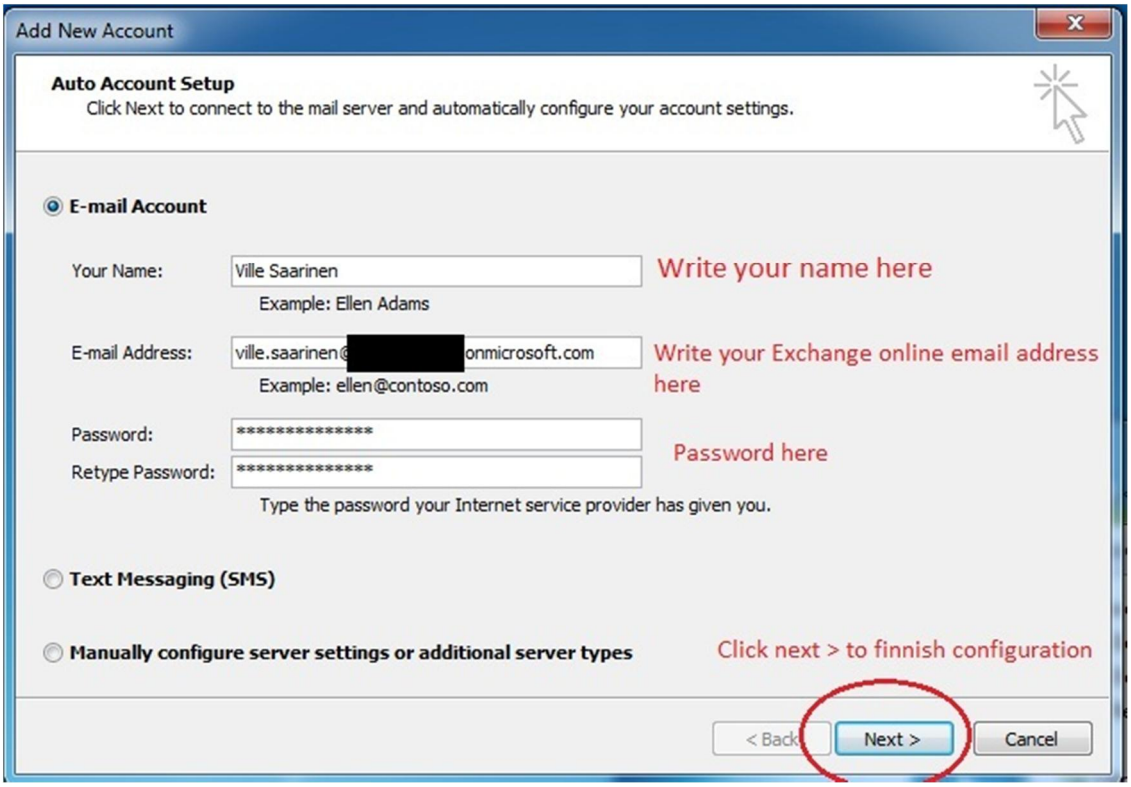
Liite 1: Sähköpostitilin lisääminen Outlook- asiakasohjelmaan

How to add email account to your outlook client

1. Open Outlook client and click File -> Add Account.



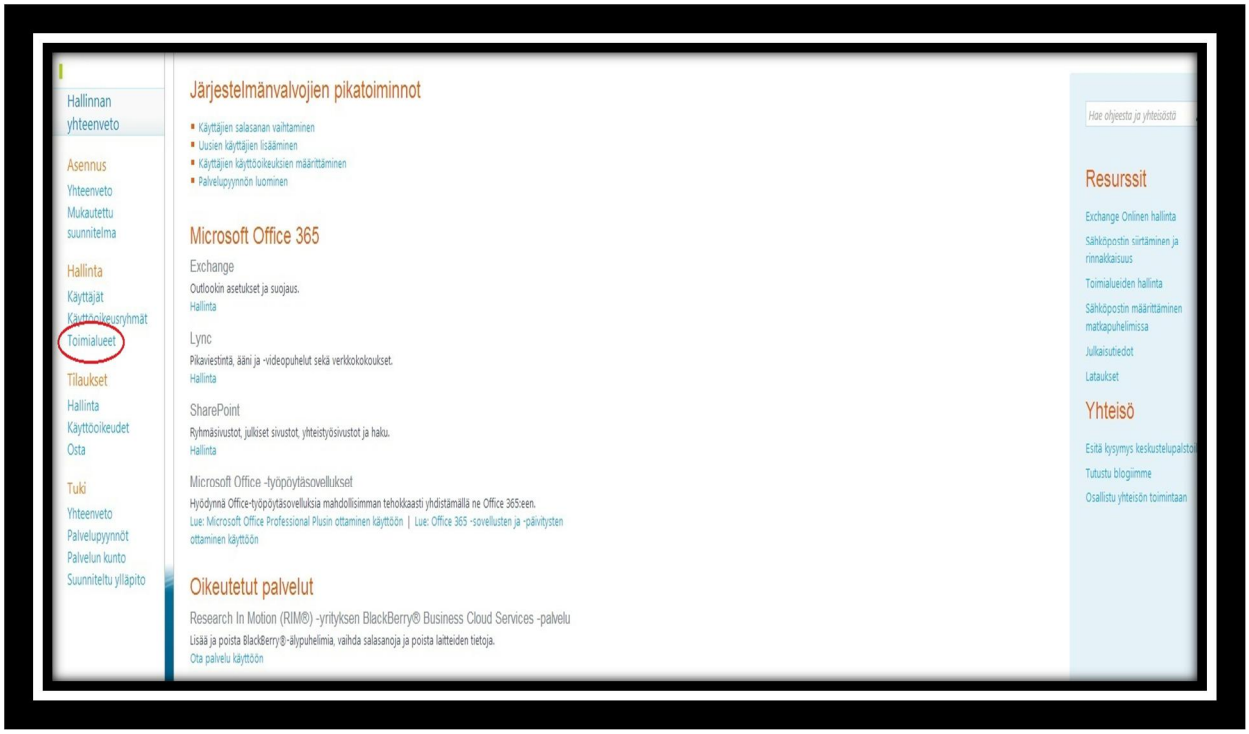
2. Setup the account information as shown in the picture below


Add New Account
Auto Account Setup
Click Next to connect to the mail server and automatically configure your account settings.
E-mail Account
Your Name:
Ville Saarinen
Example: Ellen Adams
Write your name here
E-mail Address:
ville.saarinen@[redacted]onmicrosoft.com
Example: ellen@contoso.com
Write your Exchange online email address here
Password:
Retype Password:
Password here
Type the password your Internet service provider has given you.
Text Messaging (SMS)
Manually configure server settings or additional server types
Click next > to finnish configuration
< Back
Next >
Cancel

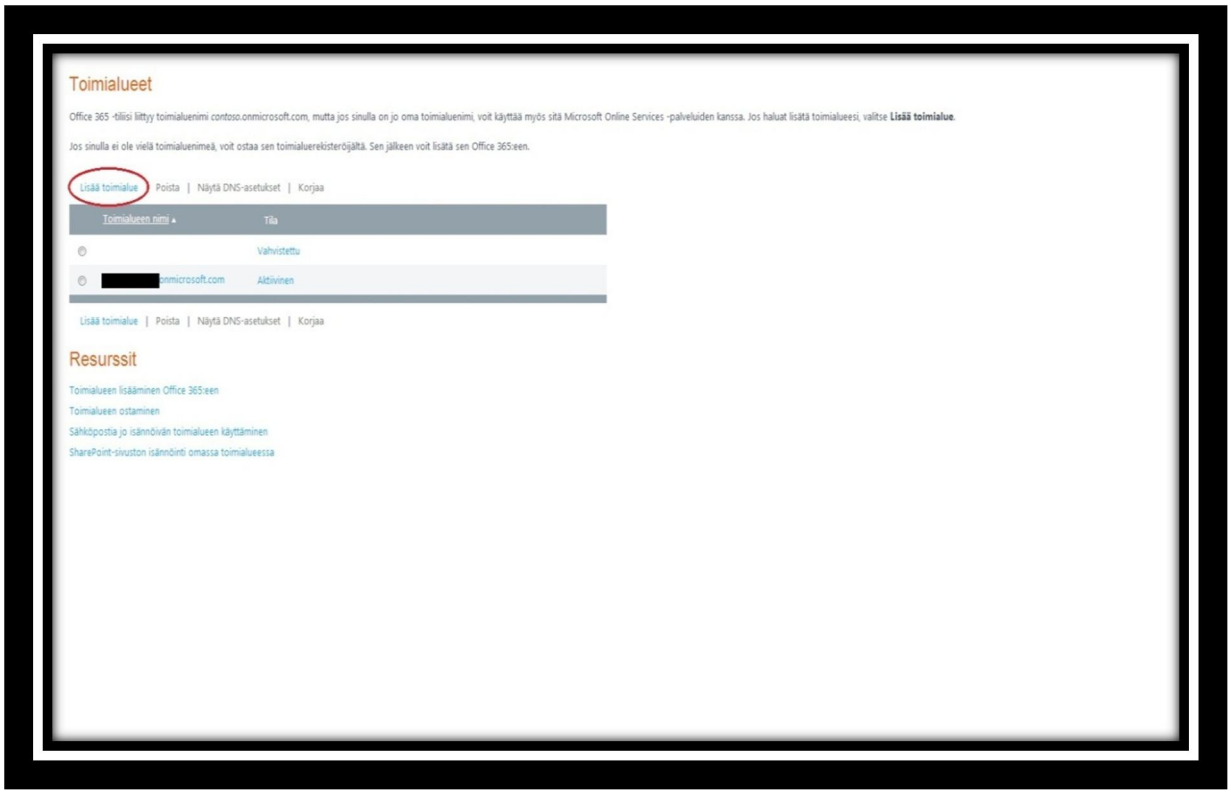
Liite 2: Toiminimen liittäminen Microsoft Office 365- pilvipalveluun.

Toimialueen lisääminen Microsoft Exchange Online-palveluun

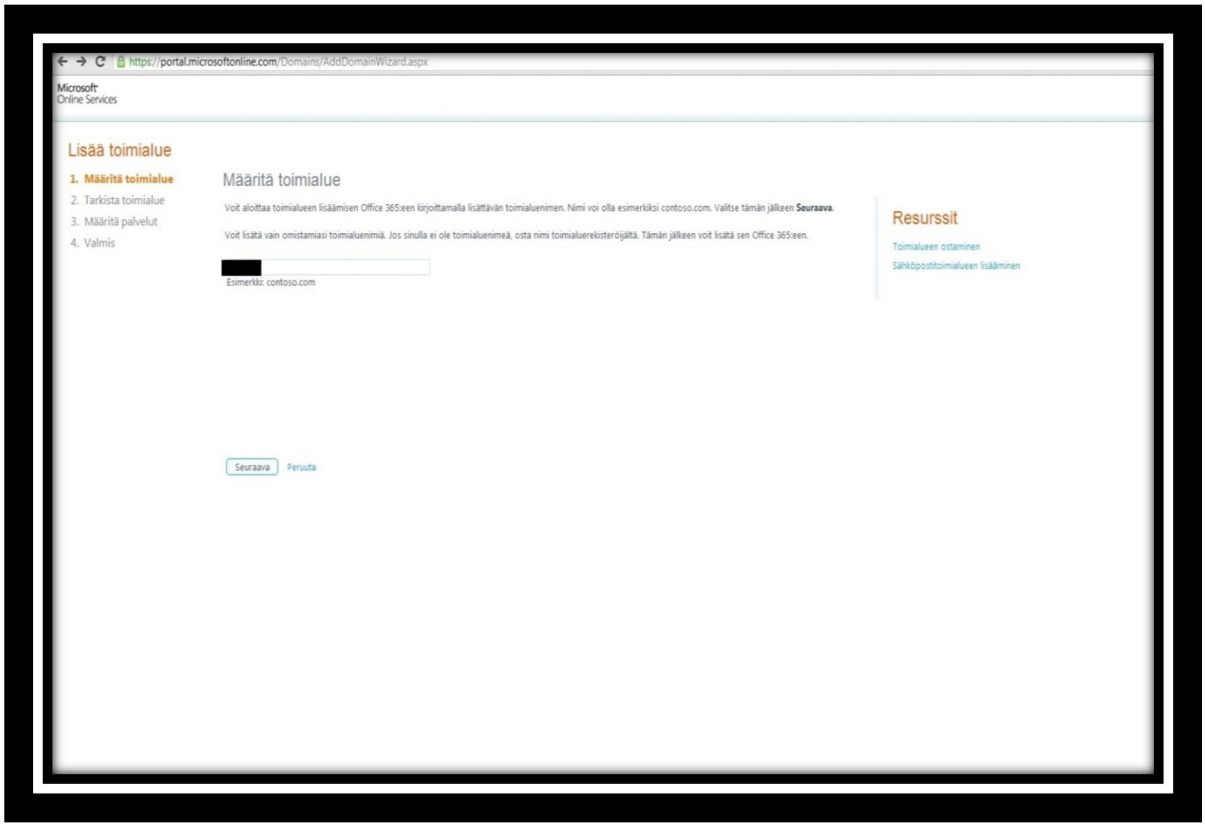
Microsoft Online Services- sivuston Järjestelmävalvoja- välilehdeltä löytyy linkki Hallinnan alla olevaan toimialueet välilehteen.



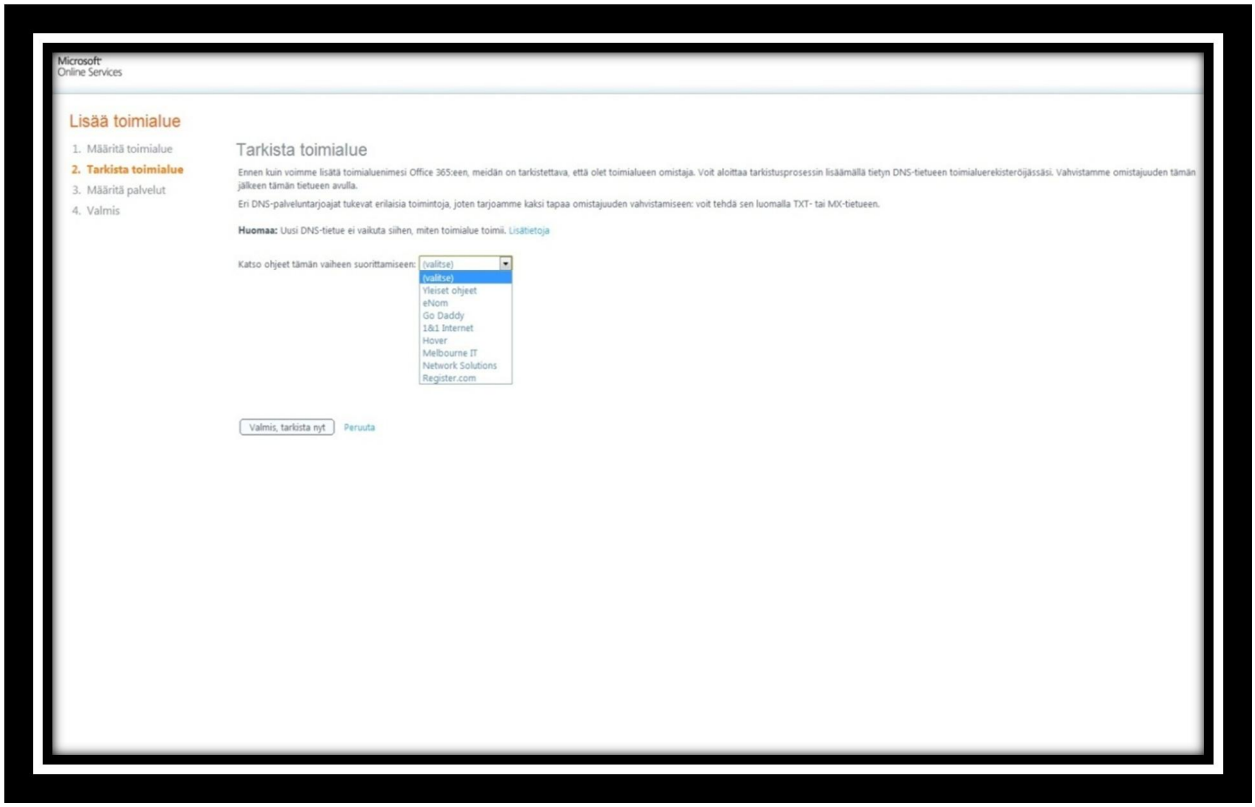
Microsoft Online Services luo automaattisesti hankinnan yhteydessä oman toimialueen muotoon esimerkkiyritys.onmicrosoft.com. Online Serviceen luodut sähköpostiosoitteet tulevat muotoon esimerkiksi etunimi.sukunimi@esimerkkiyritys.onmicrosoft.com. Toimialueet välilehdeltä valitaan kohta ”Lisää toimialue”.



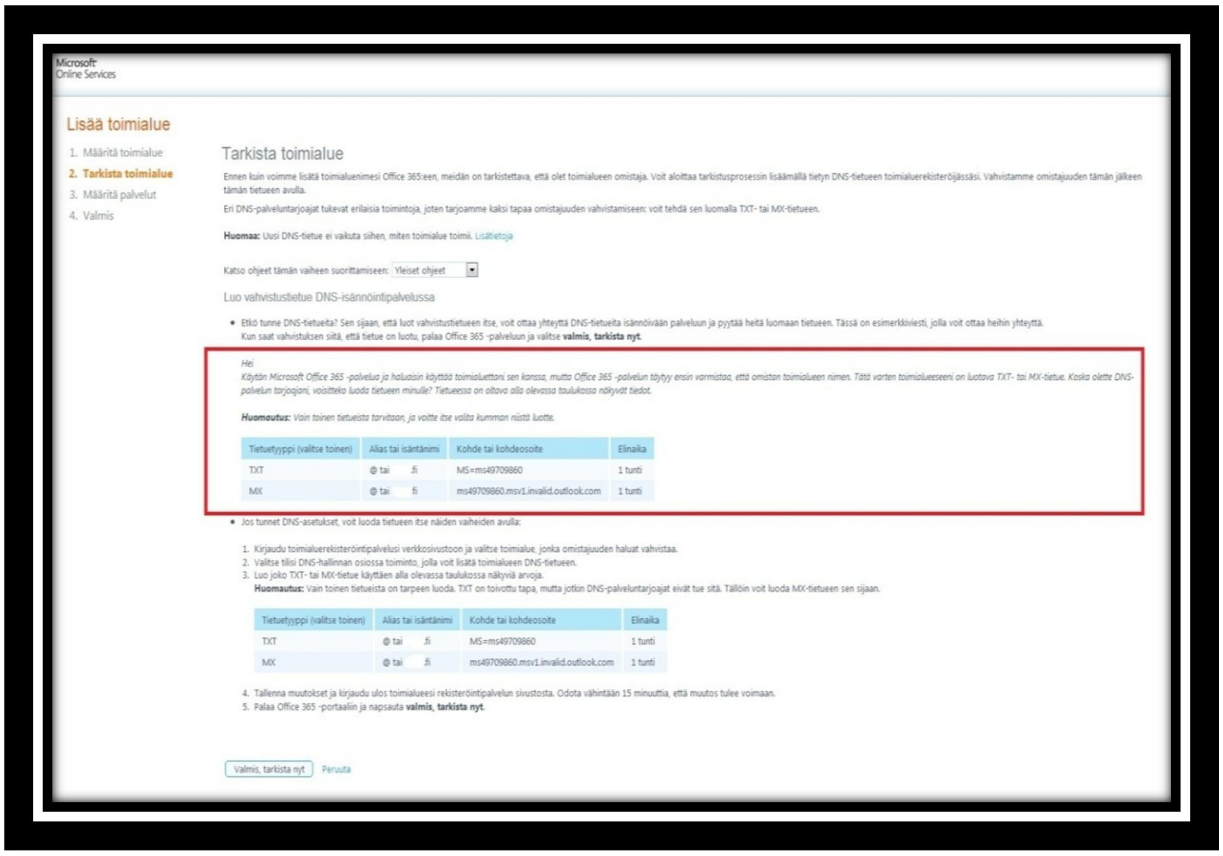
Palkkiin kirjoitetaan oman toimialue muodossa esimerkkidomain.fi. Valitse seuraava.



Microsoft Online Services vaatii toimialueen omistajuuden tarkistamisen. Tähän tarvitaan DNS-tietue DNS- palveluntarjoajalta. Online Services tarjoaa valmiiksi ohjeita eri palveluntarjoajille tietueen saamiseksi. Tässä tapauksessa valittiin ”Yleiset ohjeet”.



Tietue voidaan joko luoda itse tai se voidaan pyytää palveluntarjoajalta. Tässä tapauksessa DNS- tietue pyydettiin palveluntarjoajalta käyttämällä rajattua esimerkkisähköpostia. DNS-tietue oli lisätty palveluntarjoajan toimesta 3 päivän jälkeen. Varmistuksen saapuessa valittiin ”Valmis, tarkista nyt”. Tämän jälkeen toimialue näkyi toimialuelistassa aktiivisena. Udeen sähköpostin luominen onnistui nyt myös oman toimialueen muodossa (esim. etunimi.sukunimi@yritys.fi).


Microsoft
Online Services
Lisää toimialue
1. Määritä toimialue
2. Tarkista toimialue
3. Määritä palvelut
4. Valmis
Tarkista toimialue
Ennen kuin voimme lisätä toimialuenimesi Office 365:een, meidän on tarkistettava, että olet toimialueen omistaja. Voit aloittaa tarkistusprosessin lisäämällä tietyn DNS-tietueen toimialuerekisteröijässäsi. Vahvistamme omistajuuden tämän jälkeen tämän tietueen avulla.
Eri DNS-palveluntarjoajat tukevat erilaisia toimintoja, joten tarjoamme kaksi tapaa omistajuuden vahvistamiseen: voit tehdä sen luomalla TXT- tai MX-tietueen.
Huomaa: Uusi DNS-tietue ei vaikuta siihen, miten toimialue toimii. Lisätietoja
Katso ohjeet tämän vaiheen suorittamiseen: Yleiset ohjeet
Luo vahvistustietue DNS-isännöintipalvelussa
Etkö tunne DNS-tietueita? Sen sijaan, että luot vahvistustietueen itse, voit ottaa yhteyttä DNS-tietueita isännöivään palveluun ja pyytää heitä luomaan tietueen. Tässä on esimerkkiviesti, jolla voit ottaa heihin yhteyttä.
Kun saat vahvistuksen siitä, että tietue on luotu, palaa Office 365 -palveluun ja valitse valmis, tarkista nyt.
Hei
Käytän Microsoft Office 365 -palvelua ja haluaisin käyttää toimialuettoni sen kanssa, mutta Office 365 -palvelun täytyy ensin varmistaa, että omistan toimialueen nimen. Tätä varten toimialueeseeni on luotava TXT- tai MX-tietue. Koska olette DNS-palvelun tarjoajani, voisitteko luoda tietueen minulle? Tietueessa on oltava alla olevassa taulukossa näkyvät tiedot.
Huomautus: Vain toinen tietueista tarvitaan, ja voitte itse valita kummon niistä luotte.
Tietuetyyppi (valitse toinen) | Alias tai isäntänimi | Kohde tai kohdeosoite | Elinaika
TXT | @ tai .fi | MS=ms49709860 | 1 tunti
MX | @ tai .fi | ms49709860.msv1.invalid.outlook.com | 1 tunti
Jos tunnet DNS-asetukset, voit luoda tietueen itse näiden vaiheiden avulla:
1. Kirjaudu toimialuerekisteröintipalvelusi verkkosivustoon ja valitse toimialue, jonka omistajuuden haluat vahvistaa.
2. Valitse tilisi DNS-hallinnan osiossa toiminto, jolla voit lisätä toimialueen DNS-tietueen.
3. Luo joko TXT- tai MX-tietue käyttäen alla olevassa taulukossa näkyviä arvoja.
Huomautus: Vain toinen tietueista on tarpeen luoda. TXT on toivottu tapa, mutta jotkin DNS-palveluntarjoajat eivät tue sitä. Tällöin voit luoda MX-tietueen sen sijaan.
Tietuetyyppi (valitse toinen) | Alias tai isäntänimi | Kohde tai kohdeosoite | Elinaika
TXT | @ tai .fi | MS=ms49709860 | 1 tunti
MX | @ tai .fi | ms49709860.msv1.invalid.outlook.com | 1 tunti
4. Tallenna muutokset ja kirjaudu ulos toimialueesi rekisteröintipalvelun sivustosta. Odota vähintään 15 minuuttia, että muutos tulee voimaan.
5. Palaa Office 365 -portaaliin ja napsauta valmis, tarkista nyt.
Valmis, tarkista nyt
Peruuta