Tässä dokumentissa kuvataan Itä-Suomen Taitajat Oylle rakennetta rakennettava uusi IT-ympäristö yrityksen muuttaessa uuteen toimipisteeseen.

Palvelin ympäristön perustana toimii edessäsi oleva huippuluokan palvelin, johon on laitetoimittajan toimesta esiasennettu Windows Server 2008 R2 Standard ja Hyper-V. Alustan päälle asennetaan kaksi virtuaalipalvelinta joista toiseen tulee Windows Server 2008 R2 Standard sekä toiseen Debian GNU/Linux 5.0.4 käyttöjärjestelmä.

Windows palvelimelle asennetaan Active Directory rooli, johon luodaan jokaiselle työntekijälle omat käyttäjätunnukset. Käyttäjätunnuksilla pystyy kirjautumaan jokaiselta tietokoneelta, joka on liitettynä Windows-palvelimeen. Käyttäjätunnuksien nimeämisessä käytetään vakiomuotoa, 2 ensimmäistä kirjainta etunimestä ja 4 ensimmäistä kirjainta sukunimesä esimerkiksi Matti Mallikolla käyttäjätunnus olisi mamall

Riippumatta tietokoneesta tai käyttäjän tietokoneen sijainnista jokaiselle käyttäjälle annetaan aina sama ”Documents” –kansio ohjaamalla se käyttäjänä kotikansioon. Näin myös kaikki työdata, mikä on tallennettuna kansioon pysyy tallessa varmemmin.

Windows palvelimella asennetaan keskitetysti jokaiseen työasemaan automaattisesti Office-paketti. Outlook sähköpostiohjelma liitetään käyttäjäkohtaisesti automaattisesti palveluntarjoajalta ostettuun Exchange –palvelimeen. Tällöin informaation välitys yrityksen sisällä helpottuu, koska kaikki yhteiset tapaamiset ja sähköpostit ja puhelinluettelot siirtyy kätevästi sähköpostiohjelmiston välityksellä jokaiselle työntekijälle.

Koska jokaiseen koneeseen tulee päästä etäkäytöllä sisälle, pakotetaan group policyillä etätyöpöytä ja etäopastus-toiminnot käyttöön.

Nykypäivän tietoturvasta tullaan myös huolehtimaan palomuurilla ja virustorjunnalla. Internetpalveluntarjoajalta (ISP) tilataan ulkomaailman ja sisäverkon väliin fyysinen palomuuri, jonka he konfiguroivat yrityksen tarpeiden muikaisesti. ISPin palomuuri toteutus sisältää myös VPN toteutuksen jonka avulla yrityksen työntekijät pystyvät käyttämään sisäverkon resursseja myös maailmalta.

Kaikkiin työasemiin määritetään pakotetusti palomuuri päälle. Palvelimissa palomuuria ei pakoteta päälle, mutta se pidetään päällä. Virustorjunnasta huolehditaan keskitetysti Linux-palvelimelle asennettavalla F-Secure Policy Manager ohjelmistolla. Työasemiin jaetaan keskitetysti F-Secure Client Security sekä palvelimiin F-Secure Anti-Virus.

Koko yrityksen verkko kytketään yrityksen sisällä yhteen kytkimeen, josta lähtee yksi kaapeli palveluntarjoajan vuokrareitittimelle. Yrityksen omaan kytkimeen tehdään yksi virtuaaliverkko työasemille ja palvelimille sekä toinen kytkimen hallintaa varten. Salasanat piilotetaan konfiguraatiosta tietoturvan takia. Kytkimeen määritetään päälle telnet etähallinta.

Kaikki yrityksen HTTP-liikenne (porttiin 80) tullaan kierrättämään välityspalvelimen kautta, jonka avulla voidaan estää pääsy esimerkiksi tietyille sivustoille, jotka todetaan haitallisiksi. Liikenteen valvonta tapahtuu Linux-palvelimella. Välityspalvelinohjelmistona käytetään squid-ohjelmaa. Jokaisen käyttäjän Internet Explorer määritetään käyttämään Linux-välityspalvelinta ryhmäkäytöntöjen avulla.

Kaikille työntekijöille jaetaan jokaiseen työasemaan automaattisesti toimiston tulostin, jolle he voivat tulostaa. Tulostin tulee olemaan verkkoon liitettävä IP-tulostin. Windows palvelin jakaa myös jokaiselle koneelle automaattisesti IP-asetukset (IP, mask, gateway, dns) DHCP-palvelun avulla.

Yrityksen sisäisten infojen yms. jakamiseen on luodaan yrityksen sisäverkossa toimiva intranet-sivusto. Intranettiin tulee myöhemmin koonti yrityksen asiakkaista ja heidän ongelmistaan ja ratkaisuistaan. Kaikki työntekijöille kuuluvat asiat voidaan turvallisesti jakaa tätä kautta. Tällöin ei kaikkea tarvitse lähettää sähköpostitse ja liikennemäärät laskee verkossa. Intranet toteutetaan Linux-palvelinta käyttäen Apache-ohjelmistoa ja sinne määritetään päivitysoikeudet yrityksen markkonointiosastolle. Sekä opastetaan heille intranetin päivittämisrutiini.

Varmuuskopiot otetaan kaikista käyttäjäkohtaisista ja ryhmäkohtaisista tiedostoista viikottain verkkokiintolevylle, joka sijaitsee samassa verkossa (mutta fyysisesti toimitusjohtajan kotona) , joten tulipalon sattuessa tiedostot voidaan palauttaa.

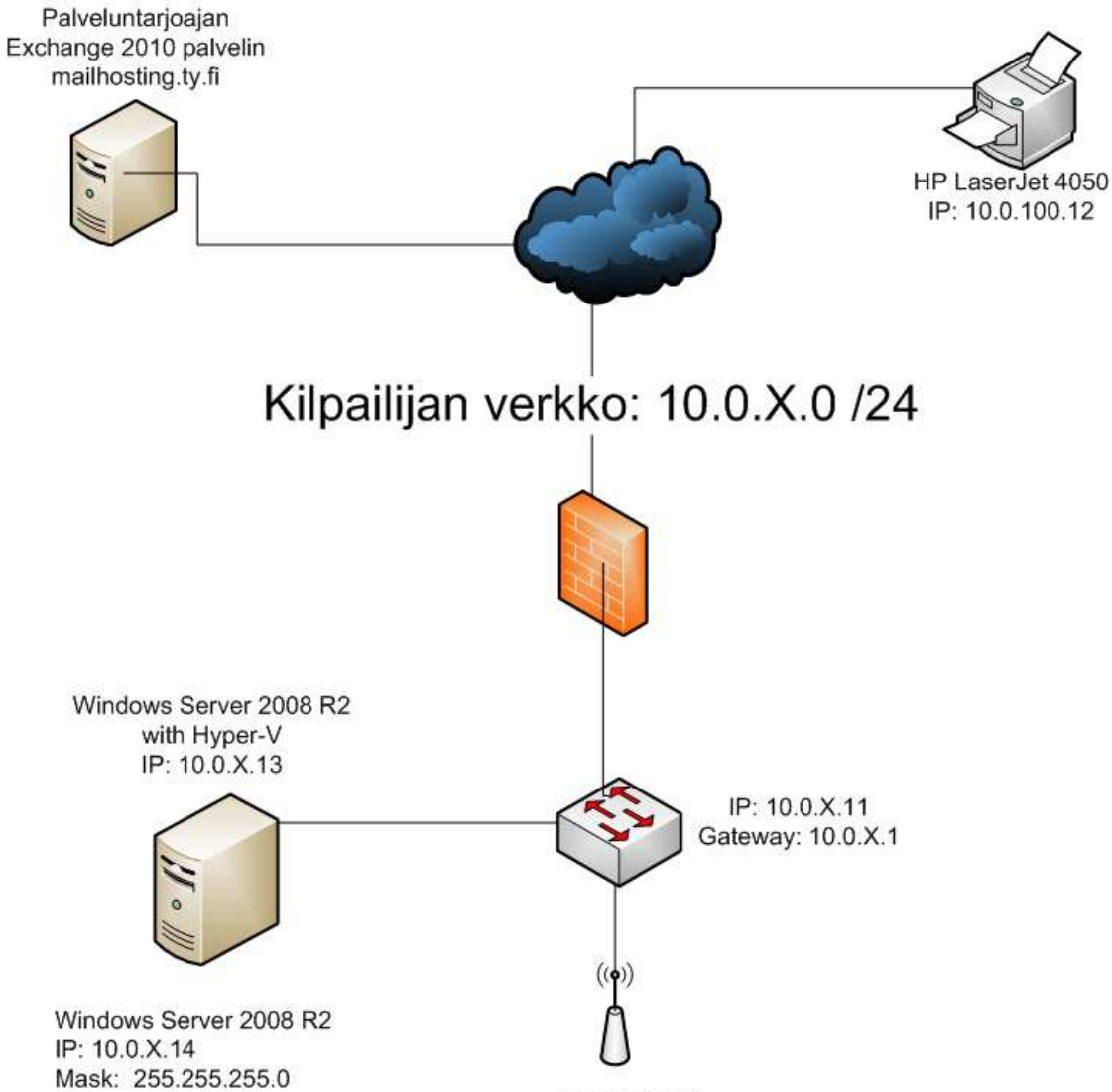
Tietomurtojen välttämiseksi tulee jokainen virheellinen kirjautuminen tallentaa virhelokiin, josta voidaan tarvittaessa lähteä jäljittämään tietomurtojen yrittäjää. Lokit tallennetaan Windows-palvelimen event-lokiin. Sekä Linux palvelimen osalta Linuxin erilliseen lokiin /var/log/auth.err -tiedostoon.

Yrityksen neuvotteluhuoneeseen asennetaan langaton verkko, johon jokainen yrityksen tietokone, jossa on langaton verkkokortti yhdistyy automaattisesti. Mitään tunnuksia kyselemättä on langaton verkko käytössä välittömästi kun kone on verkon kantoalueella. Tällöin helpotetaan tiedostojen käyttöä esimerkiksi palavereissa yms. Langattoman verkon asetukset jaetaan koneille ryhmäkäytäntöjen avulla.

Yritykseen hankittavat uudet tietokoneet asennetaan uudestaan yrityksen IT-käytäntöjä noudattaen. Koneiden asennus onnistuu vaivattomasti Windows-palvelimeen asennettavan WDS-palvelun avulla. WDS palvelimelta voidaan asentaa koneisiin automaattisesti käyttöjärjestelmät siten, että ei tarvitse kuin valita koneen malli luettelosta. WDS-palvelun käytöstä tehdään selkeät ohjeet ja siitä toteutetaan käyttökoulutus kaikille sitä tarvitseville.

Koko IT-infrastruktuuri dokumentoidaan ja dokumentoinnit tallennetaan yrityksen palvelimelle varmaan talteen. Ne myös tulostetaan toimitusjohtajan kotona olevaan kassakaappiin. Dokumentoinnista löytyy myös pääkäyttäjän tunnukset, sekä muut tarvittavat tiedot myöhempää IT-päivitystä varten, jos sellaista joskus tullaan tekemään.

Malli verkkokuva



Windows –palvelin

- Active Directory
- DNS
- DHCP
- WDS

Linux –palvelin

- Apache
- Squid
- F-Secure Policy Manager

IT-infrastruktuuri

- Layer 2 kytkin
- WLAN-tukiasema