Haaga-Helia
ammattikorkeakoulu Oy

Eri etätyömenetelmät ja niiden tietoturva

Tuomo Gustafsson

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2016

Tekijä(t)
Tuomo Gustafsson

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Eri etätyömenetelmät ja niiden tietoturva

Sivu- ja liitesivumäärä
49

Tämän opinnäytetyön tarkoituksena oli tutkia etätyöskentelyä, sen eri menetelmiä sekä näiden menetelmien tietoturvaa. Työhön on valittu kolme eri etätyömenetelmää, jotka ovat VPN-yhteys, työpöytävirtualisointi sekä pilvipalvelut osana etätyöskentelyä. Menetelmät valittiin niiden suosion sekä oman kokemuksen vuoksi.

Työn tarkoituksena on tutkia etätyötä toimistoympäristössä, jonka keskeisimpiä työvälineitä ovat erilaiset toimisto-ohjelmat, kuten tekstinkäsittelyohjelmistot, sähköpostisovellukset ja tiedostonhallintasovellukset. Tarkoituksena ei ollut laajentaa etätyön tutkimista muille aloille.

Etätyömenetelmiä lähdettiin tutkimaan käytännönläheisellä otteella, jossa jokaisen etätyömenetelmän kohdalla hyödynnettiin sille räätälöityä sovellusta tai palvelua. Sovellusten toimintaa kuvattiin painottamalla niiden toiminnassa ilmenneiden vaiheiden tietoturvaa. Testauksen lähtökohtana käytettiin kuvitteellista tilannetta, jossa etätyöskentelijän tulee päästä muokkaamaan yrityksen sisäistä tiedostoa.

Menetelmiä lähdettiin vertaamaan tietoturvalle asetettuihin tavoitteisiin tarkastelemalle sitä, kuinka hyvin ne täyttävät kunkin kohdan. Tämän lisäksi testauksen yhteydessä ilmenneitä tietoturvariskejä lähdettiin analysoimaan riskianalyysin avulla sekä kehittämään näille riskeille ennaltaehkäiseviä toimenpiteitä, joiden avulla niiden toteutumisen todennäköisyys saadaan pienentymään tai eliminoitua kokonaan.

Työtä tehtiin syyskuusta 2016 joulukuuhun 2016. Työ eteni ajallaan, eikä sitä tehdessä kohdattu suuria haasteita.

Työn tulosten avulla voitiin päätellä, että tietoturvallisin ratkaisu näistä kolmesta menetelmästä on pilvipalveluiden hyödyntäminen osana etätyöskentelyä. Tämän menetelmän kohdalla ilmeni vähiten mahdollisia tietoturvariskejä. Menetelmää valittaessa täytyy kuitenkin ottaa huomioon yrityksen omat mieltymykset. VPN-yhteys soveltuu yritykselle, joka haluaa itse olla vastuussa tiedon säilömisestä ja palveluiden ylläpidosta. Työpöytävirtualisointi pelkästään etätyötä varten ei ole viisas ratkaisu vaan sen hyödyntäminen vaatisi koko toimistoympäristön muokkausta virtuaaliseksi.

Asiasanat
etätyö, tietoturva, VPN, työpöytävirtualisointi, pilvipalvelu

Sisällys

1 Johdanto

Etätyöllä tarkoitetaan työskentelytapaa, joka ei ole ajasta tai paikasta riippuvainen. Sen ideana on tarjota työntekijälle mahdollisuus tehdä työtään itselleen parhaaksi näkemässään paikassa ja mahdollisesti myös luoda joustoa työaikojen suhteen. Etätyöskentelyn määrä on kasvanut Suomessa viime vuosikymmenien aikana tasaiseen tahtiin ja vuonna 2013 jopa neljännes suomalaisista työntekijöistä harrasti etätyötä vähintäänkin satunnaisesti. Tähän määrään kuuluvat siis päivittäin, viikoittain, kuukausittain tai satunnaisesti etätyötä tekevät. (Lyly-Yrjänäinen 2014.) Syitä etätyöskentelyyn saattaa olla monia. Joillekin esimerkiksi vilkas toimistoelämä aiheuttaa jatkuvasti keskeytyksiä työntekoon, mikä vaikuttaa merkittävästi henkilön työpanokseen. Toisille taas välimatka toimiston ja kodin välillä saattaa olla ratkaiseva tekijä, jos kilometrejä kasaantuu useita satoja päivässä. Myös globalisaatio on aiheuttanut sen, että yrityksillä saattaa olla useita toimipisteitä ympäri maailmaa, eivätkä perinteiset tapaamiset toimistolla aina enää ole mahdollisia. Projekteja hoidetaan usealla eri taholla, useassa eri paikassa. Jotta näiden tapaamisten ja projektien saumaton eteneminen olisi mahdollista, tulee yrityksen tarjota työntekijöilleen pääsy tiedostoihinsa mistä tahansa. (Työterveyslaitos ja Suomen ympäristökeskus.) Jatkuvasti kehittyvät teknologiat ja sovellukset ovat mahdollistaneet uusia keinoja toteuttaa etätyöskentelyä. Niiden soveltaminen erilaisiin työyhteisöihin on kuitenkin aina tapauskohtaista yrityksen toimintatavoista riippuen. Etätyöskentely yhdistetään yleensä vahvasti toimistotyöskentelyyn, mutta nykyään sitä hyödynnetään aina kaivostyöskentelystä leikkaussaleihin asti (Rantanen 2016). Oikeanlaista etätyöskentelymenetelmää valittaessa täytyy niin työnantajan kuin työntekijänkin punnita useita eri osa-alueita, joita ovat muun muassa käytetyn menetelmän käytännöllisyys, tietoturva, kustannukset ja käytettävän välineistön mahdollisuudet.

Tämän opinnäytetyön ideana on tutkia eri etätyöhön tarkoitettuja ratkaisuja ja käydä läpi niiden toimintaa. Opinnäytetyöhön on valittu kolme eri etätyömenetelmää, jotka ovat VPN-yhteys, työpöytävirtualisointi sekä pilvipalveluiden hyödyntäminen osana etätyöskentelyä. Nämä menetelmät valittiin erityisesti kirjoittajan oman tietämyksen ja kokemuspohjan vuoksi. Hankittujen omien kokemusten pohjalta näitä menetelmiä voidaan pitää soveltuvina etätyöskentelyyn. Erityisesti työssä on painotettu näiden menetelmien tietoturvaa sekä sitä, kuinka se on toteutettu. Tietoturvan merkitys on erityisen suuri silloin, kun arkaluontoista tietoa joudutaan kuljettamaan jatkuvasti suojaamattoman verkon ylitse. Projektin ideana on tuottaa mahdollisimman konkreettista ja helposti hyödynnettävää tietoa etätyöskentelyn eri vaihtoehdoista, jotta esimerkiksi työnantajat voivat helposti selvittää juuri heille soveltuvan etätyöskentelymenetelmän.

Raportissa käsitellään ensin etätyötä käsitteenä, kerrotaan sen taustasta ja kasvusta. Sitten tarkastellaan etätyöskentelyn hyötyjä ja haittoja käsitellään työnantajan ja työntekijän näkökulmasta. Sen jälkeen käydään tietoturvaa läpi yleisesti, sen eri osa-alueita sekä tietoturvariskien arviointiin käytettäviä menetelmiä. Myös etätyöskentelyn kannalta tärkeitä tietoturvanäkökulmia on nostettu esiin. Tämän jälkeen paneudutaan eri etätyön toteutusmenetelmiin, niiden rakenteeseen sekä toimintaan ja painotetaan erityisesti niiden toteutuksessa käytettyjä tietoturvamenetelmiä. Eri etätyömenetelmiä arvioidaan tietoturvalle asetettujen tavoitteiden kautta ja mahdollisia riskejä arvioidaan riskianalyysin avulla. Jokaista etätyömenetelmää testataan käytännössä, toteuttamalla kuvitteellinen etätyöskentelytilanne, jossa työntekijän tulee päästä käsiksi yrityksen sisäiseen tiedostoon. Testauksen avulla ilmenneille riskeille on pyritty keksimään ehkäisymenetelmiä, joiden avulla niiden toteutuminen pyritään välttämään. Pohdinnassa on käyty läpi sitä, minkälaiseen ympäristöön kukin etätyömenetelmä on otollisin sekä vertailtu näiden menetelmien positiivisia ja negatiivisia puolia.

1.1 Katsaus aiempaan tutkimukseen

Etätyötä ja sen tietoturvaa on tutkittu aiemminkin. Aihetta on käsitelty niin yksittäisten komponenttien osalta kuin myös yrityksen toiminnan näkökulmasta. Useat näistä tutkimuksista kuitenkin painottuvat jonkin tietyn menetelmän tietoturvaan. Varsinaisesti etätyöskentelyä ja sen tietoturvaa yleisesti on käsitelty vain muutamissa töissä.

Rahkola (2013) on käsitellyt työssään sekä etätyötä että sen tietoturvaa. Aihetta on lähdetty käsittelemään tietoturvan teknisiä osa-alueita silmällä pitäen ja sitä, mitä niiden toiminnassa pitää ottaa huomioon etätyöskentelyn näkökulmasta. Tavoitteena on ollut luoda ohjeistus, jonka mukaan etätyöntekijöiden tulisi toimia. Etätyömenetelmiä ei ole tässä työssä, muutamaa mainintaa lukuun ottamatta, käsitelty.

Piispanen (2006) käsittelee työssään etäkäyttöohjelmistoja käyttäjän näkökulmasta sekä selvittää niiden tietoliikenneyhteyksiä ja tietoturvaa. Työssä on annettu erityisesti painoarvoa VPN-yhteyksillä toteutetuille ohjelmistoille. Käsiteltäviä ohjelmistoja ovat Symantecin PcAnywhere, Laplink Gold sekä Citrix Metaframe. Näitä asioita käsitellään teoreettisena kirjoituspöytätutkimuksena, jossa hyödynnettiin jo valmiina olevaa tietomateriaalia. Tuloksena todetaan, että PcAnywhere ja Laplink Gold soveltuvat mikrotuki- ja palvelinhallintatehtäviin sekä etätyöskentelyyn. Niiden tietoturvan tasoa pidetään hyvin samankaltaisena. Metaframe soveltuu ohjelmistojen etäkäyttöön palvelimilta ja se sisältää on valmiiksi hyvät tietoturvayhteydet.

Hirvonen (2011) käsittelee työssään työasemavirtualisointia ratkaisuna kohdeyrityksen etätyöskentelyongelman ratkaisemiseksi. Haasteita yrityksessä esiintyy erityisesti ulkomailla työskentelevien työntekijöiden kanssa, joille on taattava toimiva työympäristö. Ratkaisua lähdettiin toteuttamaan käytännössä, jonka jälkeen sen toimivuutta arvioitiin yrityksen tarpeisiin peilaten. Tuloksena todettiin, että virtuaalijärjestelmä havaittiin erittäin hyväksi ja tehokkaaksi työkaluksi.

Myös Lieke (2012) on käsitellyt työasemavirtualisointia etätyöntekijän työasemavaihtoehtona. Asiaa lähdettiin tutkimaan suunnittelutieteellisellä otteella, jossa tietoperustan avulla valitaan yritykselle sopiva työasemavirtualisointivaihtoehto ja luodaan etenemismalli, jonka avulla työasemavirtualisointi voidaan ottaa yrityksessä käyttöön. Tuloksena todetaan, että työasemavirtualisointi on toimiva ratkaisu etätyöntekijän työasemavaihtoehtona. Jotta se on taloudellisesti kannattava ratkaisu, tulee sitä kuitenkin hyödyntää yrityksessä muutenkin kuin ainoastaan etätyömenetelmänä.

Etätyötä on siis käsitelty aiemmissakin tutkimuksissa, mutta hyvin monet näistä tutkimuksista ovat painottuneet yhteen menetelmään, jonka eri vaihtoehtoja on kartoitettu. Tässä työssä tarkoituksena on käsitellä eri menetelmiä, jolloin saadaan kattava selvitys siitä, miten ne eroavat toisistaan ja minkälaiseen käyttötarkoitukseen ne soveltuvat. Lisäksi pilvipalveluiden hyödyntäminen etätyöskentelymenetelmänä on jäänyt hyvin vähäiseksi aiemmissa tutkimuksissa.

1.2 Tärkeitä käsitteitä

C-I-A on lyhenne sanoista confidentality (luottamuksellisuus), integrity (eheys) ja availability (saatavuus), jotka ovat tietoturvan tavoitteiden kolme keskeistä komponenttia (Gibilisco & Haughn 2014).

eTyö on toinen nimitys etätyöskentelylle (Ruohomäki & Tuomivaara).

ISP (Internet Service Provider) on internet-palveluntarjoaja eli taho, joka toimittaa henkilölle verkkoyhteyden (Boswell 2016).

Mobiilityö on toinen nimitys etätyöskentelylle (Työterveyslaitos 2014).

Pilvipalvelu on tiedonhallintamenetelmä, jossa data ei sijaitse käyttäjän koneella vaan verkossa (Hanhirova 2011).

Remote Desktop on ohjelmisto, jonka avulla käyttäjä voi ottaa yhteyden omalta koneeltaan etäkoneelle, käyttäen tämän IP-osoitetta tai nimeä (Microsoft 2016).

SLA (Service Level Agreement) on sopimus, jonka avulla yritys tai yksityishenkilö ja palveluntarjoaja määrittelevät sopimusta koskevat määräykset siitä, kuinka suuren osan ajasta palvelu on käytössä sekä kuinka nopeasti ja milloin tukea saadaan vikatilanteissa (Rouse 2016).

Sovellusvirtualisointi on tapa, jolla sovellus erotellaan käyttöjärjestelmästä, jolloin se voidaan toimittaa itsenäisenä komponenttina käyttäjälle, hänen käyttöjärjestelmästään riippumatta. Sovelluksia voidaan ajaa etänä palvelimilla tai ne voidaan suoratoiston avulla toimittaa käyttäjän koneelle, jolloin ne ajetaan käytettävällä koneella. (Rouse 2016.)

TLS (Transport Layer Security) on salausprotokolla, joka tarjoaa turvallisen tavan kuljettaa tietoa salatusti ja eheästi kahden eri sovelluksen välillä (Rouse 2016).

Työpöytävirtualisointi on tapa, jolla työasema virtualisoidaan, jolloin työpöytä, kaikkine komponentteineen, sijaitsee palvelimella, jonne käyttäjä ottaa etäyhteyden päätelaitteella (Rouse 2016).

VDI (Virtual Desktop Infrastucture) on menetelmä, jolla työpöytävirtualisointi mahdollistetaan (Lovinus 2016).

Virtualisointi on tapa, jolla yhdellä fyysisellä palvelimella voidaan ajaa useampaa eri käyttöjärjestelmää, täten mahdollistaen maksimaalinen komponenttien (esimerkiksi CPU, muisti) käyttöaste (Subramanian 2016).

VLAN (Virtual Local Area Network) on tapa, jolla fyysinen tietoverkkoliikenne voidaan jakaa loogisiin osiin (Rouse 2016).

VPN (Virtual Private Network) on tapa, jolla yrityksen verkkoja tai yksittäinen käyttäjä voidaan yhdistää turvallisesti julkisen verkon yli yrityksen lähiverkkoon (Crawford 2016).

WLAN (Wireless Local Area Network) tarkoittaa langatonta lähiverkkotekniikkaa, jonka avulla laite voidaan yhdistää verkkoon ilman kaapeleita (Rouse 2010).

2 Etätyöskentely

Etätyö voidaan karkeasti määritellä työksi, joka ei ole ajasta tai paikasta riippuvainen (Työterveyslaitos ja Suomen ympäristökeskus). Tämä on kuitenkin hyvin suppea määritelmä työnteon muodolle, joka on vuosien saatossa haarautunut useaan eri muotoon. Oli työ sitten jatkuvasti etänä tehtävää, ajoittaista työmatkojen aikana tai tukena normaalille toimistotyölle, yhdistää näitä eri muotoj kuitenkin yksi asia, joka on tietotekniikan aktiivinen käyttö työnteon välineenä. (Ruohomäki & Tuomivaara; Wirén.) Kehittyneet sovellukset ja tietotekniset laitteet ovat mahdollistaneet vuosien saatossa aina vain kehittyneemmän tavan tehdä töitä. Nämä muutokset ovat myös mahdollistaneet sen, että enää työntekijä ei ole riippuvainen työpaikan ympäristöstä tehokasta työntekoa varten. (Nurmi.)

Jo 1980- luvulla kaavailtiin, että etätyö tulee yleistymään merkittävänä osana tulevaisuuden yrityksiä ja heidän tapaansa tehdä töitä. 1990- luvulla tietoteknisten välineiden määrän kasvu, kehitys ja hintojen lasku kasvattivat aina vain etätyönteon yleistymistä ja sitä hyödyntävien työntekijöiden määrää. (Heinonen 2009). Teknologian kehityksen vanavedessä kasvoi myös etätyöntekijöiden määrä aina 1990- luvun alusta vuoteen 2008, jonka jälkeen tämä kasvu on hieman hidastunut (Työolotutkimus 2008). Suomi on tutkimusten mukaan yksi Euroopan kärkimaita etätyön saralla. Haasteita etätyön tutkimiselle asettaa kuitenkin sen monet muodot, jotka toisissa tutkimuksissa saatetaan lukea etätyöksi ja toisissa taas ei. (Työterveyslaitos 2014.) Yksi merkittävä syy siihen, että Suomessa etätyöskentely on niin suosittua, johtuu sen pitkistä perinteistä tieto- ja viestintäteknologian saralla. Suomi omaksui tietotekniikan yleistymisen alkutaipaleilla hyvin nopeasti nämä uudet välineet ja menetelmät osaksi yrityksiä ja tästä syystä myös etätyöllä on ollut mahdollista kasvaa suomalaisissa yrityksissä usean vuosikymmenen ajan. (Heinonen 2009.) Etätyöntekijöiden määrä Suomessa on Työterveyslaitoksen erikoistutkija Virpi Ruohomäen mukaan pysynyt viime vuodet tasaisena ja palkansaajista noin 300 000 tekee säännöllisesti eli vähintäänkin kuukausittain etätöitä. Tämän lisäksi lähes yhtä suuri osa työntekijöistä olisi halukkaita tai kiinnostuneita tekemään etätöitä. Tähän määrään ei ole laskettu satunnaisesti eli harvemmin, kuin kerran kuukaudessa etätyötä tekeviä. (MTV 2013.) Kun kaikki etätyötä tekevät otetaan huomioon eli myös satunnaisesti sitä tekevät, nousee kokonaismäärä jopa 28 prosenttiin. Reilu neljännes suomalaisista työntekijöistä siis teki etätöitä vuonna 2013 vähintäänkin satunnaisesti. (Lyly-Yrjänäinen 2014.)

2.1 Etätyön hyödyt ja haitat

Etätyö tuo mukanaan monia eri mahdollisuuksia, mutta myös haasteita. Aloilla, joissa fyysinen läsnäolo on oleellista tai jopa välttämätöntä, etätyö ei ole vaihtoehto. Toisaalta, niillä aloilla, joilla se on mahdollista, saattaa etätyö toimina oivana rekrytointivalttikorttina ja toimistoilmapiirin parantajana. Etätyöllä on sekä hyviä että huonoja puolia, niin työnantajan kuin työntekijänkin kannalta. Näitä hyötyjä ja haittoja tullaan käsittelemään seuraavissa luvuissa.

2.1.1 Työntekijän kannalta

Työterveyslaitoksen ja Suomen ympäristökeskuksen mukaan etätyön suurin hyöty työntekijälle on työajan ja -paikan joustavuus. Etätyö mahdollistaa työntekijälle keinon tehdä työtään tavalla, joka ei ole riippuvainen siitä, missä hän sitä tekee. Tästä syystä moni valitseekin esimerkiksi oman kodin paikaksi tehdä töitä etänä, jolloin työmatkat eivät syö hetkeäkään henkilön päivästä. Ajamatta jääneet työmatkat tuovat myös taloudellisia hyötyjä, kun työntekijän ei tarvitse kuluttaa rahaa polttoaineisiin tai matkalippuihin. Joillekin taas, kuten liikuntakyvyttömille, työmatkat saattavat olla mahdottomia tai vähintäänkin haastavia, jolloin etätyö tarjoaa loistavan tavan osallistua työelämään, mikäli se muuten tuntuisi vaivalloiselta. Karsituilla työmatkoilla on iso merkitys henkilön omaan jaksamiseen, mutta myös globaalisti suuriin huolenaiheisiin, kuten ympäristöpäästöihin, joita jokainen tekemätön työmatka vähentää. Toisaalta kodin muokkaaminen omaksi työpisteeksi saattaa aiheuttaa ongelmia vapaa-ajan ja työn välille. Työajat saattavat pidentyä, kun henkilö jää huomaamatta työstämään asioita myös työajan ulkopuolella. Lisäksi selkeä jako työpaikan ja kodin välillä hämärtyy, eikä ihminen enää assosioikaan kotiaan vapaa-aikaan vaan päinvastoin.

Työntekijöitä on ihmisten tapaan moneen eri lähtöön. Joillekin toimiston tuoma hälinä ja sosiaaliset kontaktit ovat tärkeitä parhaan mahdollisen työpanoksen antamiseksi. Toisille taas oma rauha ja sitä kautta parantunut keskittymiskyky auttavat parhaan mahdollisen työtuloksen saavuttamisessa. Helsingin Sanomat raportoi omassa artikkelissaan Journal of Environmental Psychologyn tutkimuksesta, jonka mukaan avokonttorissa työskentelystä on nykyään enemmän haittaa kuin hyötyä (Tamminen 2014). Tähän tutkimukseen nojaten, varsinkin avokonttoreissa työskentelevät ihmiset hyötyvät etätyöstä muita enemmän, jos oma rauha on tärkeää. Toisaalta joillekin juuri työpaikalla saatu sosiaalinen kontakti ja interaktio muiden työntekijöiden kanssa ovat hyvinkin tärkeitä. Tästä syystä etätyötä tekevä henkilö saattaa tuntea olonsa ulkopuoliseksi, mikä puolestaan vähentää viihtyvyyttä kyseisellä työpaikalla.

Etätyö tuo mukanaan myös tietynlaisen ajallisen jouston, joka varsinkin lapsiperheiden arjessa on erityisen arvokasta. Etätyö mahdollistaa sen, että henkilö ei ole täysin sidoksissa työpaikkaansa toimistoaikoina ja pystyy auttamaan arkisissa asioissa jonkin verran enemmän. Toisaalta, etätyön sovittaminen perheen arkeen saattaa olla haaste niin työntekijälle itselleen kuin muullekin perheelle. (Työterveyslaitos ja Suomen ympäristökeskus.) Jatkuvaa kotona oloa saattaa olla haastavaa selittää lapsille ja joissain tilanteissa myös puolisolle. Helposti erehdytään luulemaan, että koska henkilö viettää päivät kotonaan, pystyy hän tuona aikana suorittamaan arkipäivän askareita, vaikka todellisuudessa aika kuluu töihin. Sari Hämäläinen (2015) oli Ylen tekemässä haastattelussa todennut juuri tämän asian yhdeksi etätyön haastavaksi puoleksi.

2.1.2 Työnantajan kannalta

Vaikka etätyö koetaankin yleensä työntekijää suosivaksi työmuodoksi, voi se hyödyntää myös työnantajaa monella tapaa. Silti monet työnantajat pitävät sitä enemmän haitallisena kuin hyödyllisenä osana työntekoa. Monet työnantajat kaipaavat myös selkeitä mittareita, joiden avulla etätyön positiiviset tai negatiiviset puolet saadaan luvuiksi. Tiettyjen osa-alueiden, kuten kohonneen työmotivaation tai työssä jaksamisen mittaaminen on kuitenkin hyvin hankalaa tai lähes mahdotonta. (Heinonen 2009.)

Todellisuudessa etäjohtamisesta saatu hyöty voi olla parhaimmillaan yksi suurimmista tekijöistä työhyvinvoinnin ja työntekijöiden tuottavuuden kannalta. Stanfordin yliopistossa tehdyn tutkimuksen perusteella työntekijöiden tuottavuus parani 13%:lla etätyön ansiosta. Tämä johtui osittain siitä, että työntekijät eivät pitäneet yhtä paljon taukoja tehdessään kotonansa töitä sekä myös siitä, että toimiston melu ja jatkuvat häiriöt vaikuttavat tehokkuuteen ja tuottavuuteen. Tämän lisäksi hyvin monet etätyöntekijät halusivat vastata heille annettuun luottamukseen ahkeralla työnteolla, mikä myös osaltaan paransi heidän työnsä laatua ja määrää. Etätyöllä on myös suora vaikutus työntekijöiden poissaoloihin. Työntekijällä on pienempi kynnys jäädä pois töistä yrityksessä, jossa etätyötä ei sallita, jos hän tuntee olonsa kipeäksi. Kotona työskenneltäessä pieni sairastelu ei välttämättä ole este työnteolle. Tämän lisäksi kotoa työskentely ehkäisee epidemia-aikoina sairastelua, mikä puolestaan on suoraan yhteydessä henkilön tekemiin työtunteihin. (Bloom, Liang, Roberts & Jing 2014.)

Etätyöskentely mahdollistaa myös kustannussäästöjä, koska yritykselle riittävät pienemmät työtilat. Henkilöiden tehdessä töitä kotoa käsin, eivät he tarvitse omaa työpistettä toimistolla, mikä lisää säästöjä niin huonekaluissa kuin myös huomioitaessa toimitilojen ko-

kotarpeita. Varsinkin isoimmissa kaupungeissa jokainen työtiloissa säästetty neliömetri saattaa parhaimmillaan vähentää kokonaiskustannuksia useilla tuhansilla euroilla. (Työterveyslaitos ja Suomen työterveyslaitos.) Tämän lisäksi etätyö on oiva valttikortti rekrytoinnissa, sillä työntekijä näkee varmasti mahdollisuuden etätyöskentelyyn positiivisena asiana. Täydellinen etätyön mahdollisuus mahdollistaa myös sen, että työntekijöitä voidaan rekrytoida mistä vain maantieteellistä sijaintia katsomatta. Se avaa mahdollisuuden suuremmalle hakijakunnalle, mikä puolestaan edesauttaa parhaan ja kyvykkäimmän työntekijän löydössä. (15Five.) Tämän lisäksi varsinkin suurkaupungeissa palkkatasot nousevat usein huomattavasti korkeammalla kuin pienemmissä asuinkunnissa. Työnantaja onnistuu saamaan säästöjä rekrytoimalla työntekijöitä myös muilta paikkakunnilta tai jopa muista maista, kun hänen ei tarvitse täyttää paikkakuntakohtaisia palkkatasoja. (Hasell.)

Alla olevassa taulukossa (taulukko 1) on esitetty etätyön hyviä ja huonoja puolia niin työntekijän kuin työnantajan kannalta. Taulukkoon on kerätty kootusti ne vahvuudet ja heikkoudet, jotka ilmenivät kappaleissa 2.1.1 ja 2.1.2.

Taulukko 1. Etätyön hyödyt ja haitat

Etätyön hyödyt ja haitat

	Työntekijä	Työnantaja
Hyödyt	- Työajan ja -paikan joustavuus - Taloudelliset hyödyt - Työrauhan parantuminen - Perhe-elämän mukauttaminen työhön helpottuu	- Työntekijöiden tuottavuus paranee - Vähemmän poissaoloja - Kustannussäästöt - Rekrytointivaltti
Haitat	- Kodin ja työpaikan erottelu hankalaa - Työaikojen pidentyminen - Sosiaaliset kontaktit vähentyvät - Koti työpaikkana vaatii ymmärtystä koko perheeltä	- Etäjohtaminen haastavaa - Tietoturva tietyissä tilanteissa työntekijän vastuulla

2.2 Etätyön osa-alueet

Etätyö tarvitsee toimiakseen ympärilleen tiettyjä elementtejä, joista osa on välttämättömiä ja toiset taas tukevat sitä ja mahdollistavat parhaan mahdollisen lopputuloksen. Kuten etätyössä muutenkin, on myös näiden välineiden kohdalla tärkeää selvittää omiin tarkoituksiin ja omaan ympäristöön sopivimmat käytännöt.

2.2.1 Laitteisto

Tärkeimpänä etätyön komponenttina voidaan pitää siihen tarvittavaa laitteistoa. Sen tarkoitus on mahdollistaa työnteko yhtä vaivattomasti niin toimistolla kuin sijainnissa, jossa etätyötä tehdään. Pekkola ja Uskelin (2004) toteavat, että yleensä laitteiston hankinta on työnantajan vastuulla, mutta esimerkiksi freelancer-tyyppiset työntekijät saattavat myös käyttää omia laitteitaan, koska hyvin usein tämän kaltaiset työntekijät työskentelevät samanaikaisesti usealle eri yritykselle. Näissä tilanteissa työntekijän kannalta on yksinkertaisempaa, että käytössä on vain yksi laite, jolloin myös tiedonhallinta helpottuu. Laitteistoon liittyvät päätökset ovat yleensä asioita, jotka työnantaja ja työntekijä sopivat keskenään työsuhteen alkaessa. Tämän lisäksi sovitaan usein myös laitteistojen asennuksesta ja huollosta. Yrityksen laitteistojen käyttö helpottaa muun muassa tietoturvan ylläpitoa, koska työnantaja pystyy asettamaan näiden laitteiden tietoturvatason heille sopivaksi. Etätyö ei millään tavalla rajoita työntekijän yksityisyyden suojaa. Tästä syystä työnantajalla ei ole oikeutta alkaa valvomaan etätyötä tekeviä henkilöitä tai heidän laitteitaan muita tarkemmin. Myös työntekijä on vastuussa tietoturvasta siinä määrin, että hänen on noudettava ja täytettävä työnantajan määrittelemät tietoturvaohjeet. Jos työnantajan laitteistoa käytetään muuhun, kuin työasioiden hoitoon, on syytä sopia selvät pelisäännöt siitä, mihin niitä saa käyttää.

Fyysisten laitteiden lisäksi työnantaja saattaa olla myös vastuussa riittävän tiedonsiirtonopeuden järjestämisestä etätyöskentelyn pääasialliseen sijaintiin. Tämä velvollisuus on usein vahvasti riippuvainen siitä, onko etätyöskentely täyspäiväistä vai vain osa-aikaista. Tiedonsiirrolla ja toimivalla verkkoyhteydellä on nykyaikaisessa etätyöskentelyssä hyvin suuri merkitys. Tarvittavat tiedostot ja ohjelmistot ovat yhä useammin selainpohjaisia tai pilvipalveluita, joiden toiminta ja käyttö edellyttävät verkkoyhteyttä. (Pekkola & Uskelin 2004.) Tilastokeskuksen vuonna 2015 toteuttamassa tutkimuksessa kävi ilmi, että kyselyyn vastanneista yrityksistä suosituimpia pilvipalveluita yrityksissä ovat sähköpostiin, tiedostontallennuksiin ja toimisto-ohjelmiin keskittyneet ohjelmat eli juuri ne ohjelmat, joita etätyöskentelyssä eniten tarvitaan. (Tilastokeskus 2015.)

2.2.2 Ohjelmisto

Toimiva etätyö tarvitsee ympärilleen myös oikeanlaiset ohjelmistot. Koska perinteiset kasvokkain suoritettavat tapaamiset eivät etänä onnistu, täytyy ne korvata tai toteuttaa jollakin muulla tavalla. Etänä työskenneltäessä esimerkiksi saman projektin jäsenet eivät välttämättä ole tavoitettavissa samaan aikaan, jolloin kokouksissa jaettu aikataulutus tai tilannekatsaus täytyy saada myös heidän tietoisuuteensa jollakin tavalla.

Erätyöskentelyn tärkeimpinä sovelluksina voidaan pitää videoneuvottelu-, projektinhallinta-, viestintä- ja tiedostonhallintasovelluksia. Erityisesti sähköpostin käytön merkitys korostuu etänä työskenneltäessä. Erilaiset pilvipalvelut ovat vaikuttaneet etätyöskentelyn arkeen oleellisesti tuomalla monet yllä mainituista sovelluksista selainpohjaisiksi, mikä mahdollistaa niiden käytön mistä tahansa verkkoyhteydellä varustetusta sijainnista. Muun muassa Microsoftin tarjoama Office 365 sovelluspaketti tarjoaa käyttäjälle käytännössä valmiin kokonaisuuden, jonka avulla etätyöskentely toimii vaivattomasti. Ohjelmisto tarjoaa käyttäjälle sähköpostisovelluksen, tekstinkäsittelyohjelmiston, erilaisia viestintäsovelluksia, tiedostonhallintaa helpottavia sovelluksia sekä projektinhallintaohjelmiston. Samankaltaisia ohjelmistopaketteja löytyy myös muun muassa Googlelta nimellä Google Apps for Work. Paketti tarjoaa Office 365 tapaan muun muassa sähköpostisovelluksen, tiedostonhallinta-, viestintä- sekä tekstinkäsittelyohjelmiston. Vaihtoehtoja siis löytyy, mutta yleensä käytettävät ohjelmistot eivät luonnollisesti ole yksittäisen käyttäjän päätettävissä vaan niissä noudatetaan yrityksen yleistä linjausta. (Huikkola 2016; Walden 2015.)

Perinteisten toimisto-ohjelmien lisäksi etätyössä vaaditaan myös ajoittain niin sanottuja alakohtaisia ohjelmistoja. Näillä ohjelmistoilla tarkoitetaan sovelluksia, jotka on kehitetty ainoastaan kyseistä työtehtävää tai toimialaa varten. Verkkopohjaisten sovellusten suurin ero tavallisiin sovelluksiin on se, että niitä voidaan käyttää verkon yli, sen sijaan, että ne ladattaisiin käyttäjän koneelle (Nishad 2015). Tämän kaltainen toiminta sovelluksessa tekee siitä mainion juuri etätyöskentelyyn, koska sen hyödyntämiseksi tarvitaan vain verkkoyhteys.

2.2.3 Johtaminen ja viestintä

Etätyöskentelyn johtaminen poikkeaa omalla tavallaan perinteisestä johtamisesta, koska alaiset eivät päivittäin ole fyysisesti läsnä. Tämän takia onkin erityisen tärkeää, että etätyöskentelyn säännöistä sovitaan hyvin tarkasti, jotta sekä työntekijä että työnantaja ovat selvillä siitä, minkälaiset velvoitteet kummallakin osapuolella on. Etätyön säännöistä sopiminen poikkeaa eri yrityksissä monellakin eri tapaa. Joissakin yrityksissä kaikille työntekijöille on annettu samanlaiset linjaukset koskien etätyötä, kun taas toisissa työyhteisöissä etätyöstä voidaan sopia esimerkiksi oman työryhmän kesken. (Hervasti 2016.)

Etätyön johtamisen tärkeimpänä kulmakivenä pidetään luottamusta alaisiin. Esimiehen on luotettava siihen, että hänen alaisena tekevät töitä sovittuna aikana, suorittavat sovittuja tehtäviä ja priorisoivat asiat oikein. Hyvin usein työntekijä haluaa vastata tähän luottamukseen, mikä näkyy tehostuneena työteolla. Jotta etätyö tuottaa haluttuja tuloksia tulee työtehtävät rajata ja selkeyttää työntekijälle entistä paremmin. Tällöin hänen on helppo jaksottaa omaa päiväänsä ja hyvällä omalla tunnolla todeta tehtävän olevan suoritettu. Etätyö ei siis ole vain perinteistä esimiesjohtamista vaan työntekijän on osattava myös johtaa itse itseään, jotta työskentely olisi mahdollisimman tuottoisaa ja tavoitteiden mukaista. (Rokka 2014; Janhonen 2014.)

Etäjohtamisen mukana korostuu myös viestinnän merkitys niin esimiehen ja alaisen kuin esimerkiksi samassa projektiryhmässä olevien työntekijöiden välillä. Koska etätyöntekijät ovat harvoin fyysisesti samassa tilassa läsnä, on tärkeää, että ajantasaiset tiedot, päivitykset ja muutokset liikkuvat työntekijöiden välillä saumattomasti ja mahdollisimman nopeasti. Tiedonkulun haasteet ovat olleet aina läsnä niin perinteisissä toimistoympäristöissä kuin etätöissäkin, mutta etätyössä sen puute korostuu entisestään, koska asioista ei kuule kahvikoneen ääressä tai sattumalta käytävällä. Esimiehen on myös pystyttävä tavoittamaan ja johtamaan alaisiaan, vaikka he eivät fyysisesti lähellä olekaan. Tämä vaatii aktiivista otetta esimieheltä sekä siihen soveltuvia kanavia, joiden kautta tieto saadaan välitettyä. Esimiehen täytyy aktiivisesti pyrkiä seuraamaan ryhmänsä työn etenemistä ja sen tuloksia. (Koivuniemi 2015; Vilkman 2016.)

3 Tietoturva

Tietoturvan oikeanlainen suunnittelu ja hoito ovat tänä päivänä elintärkeää yritykselle (Harju 2010). Pietikäisen (2013) mukaan tietoturvajärjestelyjen tarkoituksena on varmistaa, että yrityksen tietojärjestelmät, tietoaineistot ja palvelut ovat aina saatavilla, oikeassa muodossa, niille henkilöille, joilla tietoihin kuuluu olla pääsy. Ulkopuolisilta pyritään evää-mään mahdollisuus päästä tietoihin käsiksi, minkä kautta niitä voitaisiin muuttaa tai poistaa. Tiedot pyritään myös pitämään tietoturvajärjestelyjen avulla luotettavina, mikä tarkoittaa, että ne ovat ajantasaisia ja oikeita. Mahdolliset riskit, kuten haittaohjelmat, erilaiset viat laitteistoissa tai ohjelmistoissa sekä häiriötilanteet pyritään ennaltaehkäisemään tietoturvan avulla. Tällä hetkellä yhteiskunnan toiminta on aina vain enemmän riippuvainen tietojärjestelmistä ja tiedonsiirrosta. Tämän lisäksi Pietikäinen (2013) toteaa, että harva organisaatio on enää vastuussa pelkästään omasta tietoturvastaan vaan verkostoituneessa ympäristössä useat tahot saattavat olla linkitettyjä toisiinsa. Tietovuodot yrityksessä saattavat siis vaarantaa omien tietojen lisäksi myös esimerkiksi kumppaniyritysten arkaluontoiset tiedot.

Tietoturvaa voidaan pitää myös jokaisen yksittäisen työntekijän vastuuna. Kyse ei ole ainoastaan teknologiasta eli ohjelmistojen sekä laitteiden suojauksesta, myös työntekijöiden oikeanlainen käytös on oleellinen osa hyvin hoidettua tietoturvaa. Suuryritysten on mahdotonta valvoa jokaisen työntekijän jokaista painallusta ja tästä syystä on ensisijaisen tärkeää, että yrityksen tietoturvalinjaukset ja -määräykset tehdään selväksi kaikille. (Anders Innovations 2013.) Hyvin suunniteltu ja rakennettu IT-infrastruktuuri edesauttaa työntekijöiden velvollisuutta suojata arkaluontoinen tieto asiaan kuuluvalla tavalla. Tästäkin huolimatta tietoturva on aina yhtä hataralla pohjalla, kuin yhteisön heikon lenkki. (Pietikäinen 2013.)

Tietoturvan parantaminen lähtee riskien tunnistamisesta sekä niiden todennäköisyydestä ja vaikutuksista. Kun mahdolliset tietoturva-aukot on havaittu, ne tulee arvioida. Tähän voidaan käyttää alla olevaa taulukkoa (taulukko 2). Riskien arvioinnin jälkeen on tärkeää löytää tapoja, joilla ne voidaan minimoida tai eliminoida kokonaan. Jos havaittuja riskejä tai riskiä ei pystytä kokonaan ehkäisemään tai saattamaan sille tasolle, että toteutuessaan ne eivät vaaranna yrityksen tietoturvaa merkittävästi, tulee riskin mahdollisesti aiheuttava toiminta kieltää. (VAHTI 2009.)

Taulukko 2. Riskianalyysi (VAHTI 2009)

Riskinalyysi

	Seuraukset		
Todennäköisyys	Vähäinen	Haitallinen	Vakava
Epätodennäköinen	1 Merkityksetön riski	2 Vähäinen riski	3 Kohtalainen riski
Mahdollinen	2 Vähäinen riski	3 Kohtalainen riski	4 Merkittävä riski
Todennäköinen	3 Kohtalainen riski	4 Merkittävä riski	5 Sietämätön riski

Riskianalyysin ideana on arvioida tunnistetut riskit sen perusteella, kuinka todennäköisiä ne ovat ja minkälaisia seurauksia ne aiheuttavat toteutuessaan. Taulukon perusteella saatuja tuloksia voidaan arvioida seuraavasti (Työsuojeluhallinto 2013, 7-8):

1. **Merkityksetön riski** ei aiheuta suuria toimenpiteitä, eikä siihen ole tarvetta puuttua.

2. **Vähäinen riski** ei vaadi ennalta ehkäiseviä toimenpiteitä, mutta voidaan harkita ratkaisuja riskin poistamiseen tavalla, joka ei aiheuta yritykselle suuria taloudellisia kustannuksia.

3. **Kohtalainen riski** aiheuttaa toimenpiteitä, mutta edelleen riskin eliminoinnista aiheutuvat toimenpiteet tulee mitoittaa siten, ettei niiden toteuttamisesta aiheudu suurta taloudellista tai ajallista menetystä.

4. **Merkittävä riski** aiheuttaa yritykselle niin suuren vaaran, että työtä ei saa aloittaa, ennen kuin riskin toteutumisen todennäköisyyttä tai siitä aiheutuvaa vaaraa on selkeästi pienennetty. Jo käynnissä olevan työn kohdalla riski tulisi eliminoida mahdollisimman nopeasti. Tämän tason riskeihin on syytä sijoittaa jo mahdollisia resursseja.

5. **Sietämätön riski** tulisi paikata tai korjata jo ennen kuin mitään riskin mahdollisesti aiheuttavia toimenpiteitä on aloitettu. Jos riskiä ei ole mahdollista poistaa, tulisi kaikki riskin laukaisevat toimenpiteet kieltää täysin.

3.1 Tietoturvan eri osa-alueet

VAHTI (2004) on tehnyt ohjeistuksen, jonka mukaan tietoturva jaetaan kahdeksaan eri osa-alueeseen. Tämän jaottelun perusteella tietoturvan rakentaminen, kehittäminen ja arviointi onnistuvat helpommin. Nämä kahdeksan osa-aluetta ovat:

1. **Hallinnollinen tietoturvallisuus**, jolla tarkoitetaan tietoturvan kokonaisvaltaista suunnittelua ja toteutusta aina organisaatiojärjestelyistä henkilöstön ohjeistukseen, koulutukseen ja valvontaan. Johdolla tulee olla tieto asiaankuuluvista järjestelmistä ja niiden riskeistä, jonka pohjalta he suunnittelevat, valtuuttavat ja resursoivat yrityksen tietoturvatyön.
2. **Henkilöstöturvallisuudella** tarkoitetaan henkilöstön roolituksia, vastuita ja tietoturvaohjeistuksia. Tällä varmistetaan, että jokainen työntekijä on tietoinen omasta roolistaan ja siihen liittyvistä tehtävistä sekä on sisäistänyt yrityksen tietoturvamääräykset, joiden mukaan tulee toimia. Myös rekrytointivaiheessa on tärkeää selvittää tehtävään parhaiten soveltuva henkilö, jonka osaaminen vastaa tehtävän kuvausta mahdollisimman hyvin.
3. **Fyysinen turvallisuus** sisältää muun muassa henkilöstön, laitteiden ja toimitilojen suojauksen. Ideana on luoda turvallinen ympäristö, joka on suojassa ilkivallalta ja esimerkiksi palovahingoilta. Erityisesti yrityksen palvelimet on syytä sijoittaa ja suojata siten, että mahdollisen vahingon sattuessa koko yrityksen toiminta ei lamaannu.
4. **Tietoliikenneturvallisuus** kattaa tiedonsiirtoon käytettävät tietoturvamekanismit. Sitä pyritään ylläpitämään laitteistojen ja siirtoyhteyksien hallinnalla sekä pääsynvalvonnalla.
5. **Laitteistoturvallisuus** on vastuussa yksittäisten laitteiden, kuten tietokoneiden turvallisuudesta, toiminnasta ja huollosta. Ideana on, että laitteiden hallinnointi on mahdollisimman selkeää, eivätkä poikkeustilanteet estä työntekoa.
6. **Ohjelmistoturvallisuus** sisältää nimensä mukaisesti ohjelmistoihin ja käyttöjärjestelmiin liittyvän tietoturvan. Se pitää sisällään erilaiset autentikointimenetelmät, joilla estetään luvaton pääsy järjestelmiin, sovellusten käyttöasteen ja -toimien seurannan sekä ohjelmistoihin liittyvän ylläpidon ja päivitykset.
7. **Tietoaineistoturvallisuus** tähtää muun muassa asiakirjojen ja tiedostojen tietoturvan edistämiseen. Tällä pyritään hallitsemaan, käsittelemään, säilyttämään ja hävittämään tietoaineistot asiaankuuluvalla tavalla.
8. **Käyttöturvallisuus** pyrkii takaamaan laadukkaat tuki-, ylläpito-, kehittämis- ja huoltotoimet nykyaikaisessa maailmassa, jossa nämä toimet on ulkoistettu tai se on suunnitteilla. Vaikka fyysiset laitteet tai ohjelmistot eivät enää sijaitsisi käyttäjän kanssa samassa sijainnissa, on niiden käytön tietoturva silti pyrittävä optimoimaan.

3.2 Tietoturvan tavoitteet

Tietoturva on jaettu edellä mainittuihin osa-alueisiin syystä. Tämän jaottelun avulla suurien kokonaisuuksien hallinta sujuu helpommin, kun ne voidaan jakaa pienempiin komponentteihin. Jaottelu takaa sen, että yrityksen tietojärjestelmiä pystytään tarkkailemaan useasta eri näkökulmasta, mikä takaa parhaan mahdollisen lopputuloksen ja mahdollisimman turvallisen ympäristön. Kaiken tämän takana on tavoite täyttää tietoturvan tavoitteet, jotka voidaan jakaa kuuteen eri päämäärään. (VAHTI 2004.) Näistä kolme ensimmäistä muodostavat tunnetun CIA-säännön, joka on saanut nimensä tavoitteiden englanninkielisten käännösten ensimmäisistä kirjaimista ja jälkimmäiset kolme ovat ajan saatossa täydentäneet näitä teknologian ja ohjelmistojen kehityksen myötä. Järvisen (2002, 22–23) mukaan tietoturvan tavoitteet voidaan jakaa seuraavasti:

1. **Luottamuksellisuus (confidentality)**, jolla pyritään estämään tiedon ajautuminen ulkopuolisille tahoille tai sellaisille henkilöille, joilla ei kuuluisi olla mahdollisuutta päästä tietoon käsiksi.
2. **Eheys (integrity)**, jolla pyritään takaamaan tiedon alkuperäisen muodon muuttumattomuus. Ideana on, että käyttäjä voi olla varma siitä, että hänen saamansa versio on oikeassa muodossa ilman, että siihen on päässyt kukaan kajoamaan käsittelyn, siirron tai käytön aikana.
3. **Saatavuus (availability)**, jolla pyritään takaamaan käyttäjän mahdollisuus päästä tietoon käsiksi juuri silloin, kun hän itse sitä kokee tarvitsevansa. Erilaiset palvelunestohyökkäykset tähtäävät juuri saatavuuden vaarantamiseen.

   Yllä mainittuja tavoitteita voidaan täydentää seuraavilla:

4. **Todentaminen (authentication)**, jolla pyritään varmistumaan siitä, että tietoon käsiksi pyrkivä henkilö, laite tai palvelu on se, joka hän väittää olevan. Todentamisen tukena toimivat muun muuassa salasanat, joiden oletetaan olevan asianmukaisen henkilön hallussa.
5. **Pääsynvalvonta (access control)**, jolla pyritään varmistamaan, että henkilöllä tai palvelulla on hallussaan tarpeelliset tiedot, joiden avulla hänelle voidaan myöntää pääsy tietoihin. Pääsynvalvontaa toteutetaan yleensä käyttäjätunnuksen sekä salasanan avulla järjestelmän omasta toimesta.
6. **Kiistämättömyys (non-repudiaton)**, jolla pyritään varmistumaan siitä, että tapahtuman osapuolet ovat ainoastaan niitä henkilöitä tai palveluita, joilla on lupa olla osallisena tiedonsiirrossa. Tämän avulla osapuolet eivät voi kiistää osallisuuttaan tapahtumaan.

Vaikka tarkoituksena olisikin täyttää niin monta näistä tavoitteista kuin mahdollista, toteaa Järvinen (2002, 22) myös, että tavoitteet ovat keskenään ristiriitaisia. Tärkeää olisi pyrkiä täyttämään vähintään yllä olevan listauksen kolme ensimmäistä tavoitetta eli CIA-sääntö.

3.3 Etätyöskentelyn tietoturva

Etätyöskentelyn tietoturva on monella tavalla haastava osa-alue, koska työnantaja ei voi valvoa sitä, minkälaisissa olosuhteissa työtä tehdään. Tästä syystä etätyöskentelyn tietoturva ei ole ainoastaan työnantajan vastuulla vaan myös työntekijän on oltava selvillä siitä, minkälaisia toimintatapoja tulee noudattaa. Etätyöskentelyn tietoturvasta sovitaan yleensä yrityskohtaisesti ja jokaisella on oma tapansa saada työntekijä ymmärtämään ja tämän myötä noudattamaan annettuja tietoturvaohjeita etätyöskentelyssä. Yleensä työntekijä sitoutuu jo työsopimusta allekirjoittaessaan noudattamaan yrityksen tietoturvaohjeistusta sekä salassapito- ja vaitiolovelvollisuutta. (Castrén 2014.)

Joissakin yrityksissä voidaan myös luoda erikseen etätyötä koskevat tietoturvapolitiikka. Tämän politiikan valmistelu tulisi tehdä yhteistyössä johdon ja tietohallinnon kesken. Tällä tavalla sopimukseen saadaan kaksi eri puolta. Tietohallinto tarjoaa yksityiskohtaisia ja käytännönläheisiä ohjenuoria etätyöskentelyn teknisestä puolesta niin järjestelmien kuin laitteistojen osalta. Johto puolestaan pystyy tarjoamaan kokonaisvaltaisen viitekehyksen sille, missä olosuhteissa etätyötä saa ja halutaan tehdä. Lopullinen valvonta ja toteutus ovat kuitenkin johdon tehtäviä. (VAHTI 2009.) VAHTI (2009) neuvoo, että etätyöskentelyyn laaditussa politiikassa voidaan käsitellä esimerkiksi seuraavia asioita:

1. Ketkä saavat tehdä etätyötä ja millaista etätyötä he saavat tai eivät saa tehdä.
2. Saako etätyöhön käytettäviä järjestelmiä käyttää miltä tahansa laitteelta?
3. Etätyön käyttäjätuki.
4. Onko tietoaineistojen käsittely kolmansien osapuolten suunnittelemilla ohjelmistoilla sallittua?
5. Ajankohta, jolloin etätyötä saa tehdä.
6. Etätyöhön käytettävä laitteet ja niiden vaatimukset, kuten ohjelmistot ja fyysiset komponentit.
7. Yhteysmuodot ja niiden turvatoimet.
8. Etäkäyttäjien pääsynvalvonta.

Turvallisen etätyöskentelyn pohjana voidaan pitää selkeää politiikkaa ja ohjeistusta. Tämän lisäksi molempien osapuolten on kannettava vastuu omasta tekemisestään. Työnantajan vastuulla on tarjota työntekijälle riittävä koulutus etätyöskentelyyn sekä varmistua siitä, että tekniikka ja ohjeistus ovat kunnossa. (Viestintävirasto 2015.) Etätyöskentelyn koulutuksen ei tarvitse olla monimutkaista ja se voidaan hyvin sisällyttää muiden koulutusten yhteyteen. Koulutuksessa olisi hyvä käydä läpi muun muassa etätyön käytännön järjestelyt liittyen laitteistoihin ja ohjelmistoihin, etätyöhön liittyvät ohjeet ja suositukset, yleisimmät etätyön tietoturvallisuusongelmat sekä toiminta niiden sattuessa ja etätyön tukipalvelut. (VAHTI 2009.) Työnantaja voi myös tarpeen vaatiessa valvoa etätyöskentelyä esimerkiksi lokiseurannalla tai verkkoliikennettä tarkkailemalla (Mustonen 2014). Tämä

tulee kuitenkin tehdä tavalla, joka ei loukkaa työntekijän yksityisyydensuojaa (VAHTI 2009).

Työntekijä puolestaan on vastuussa siitä, että hän toimii annettujen ohjeiden mukaisesti eli noudattaa joko erikseen laadittua etätyöskentelyn tietoturvapolitiikkaa tai työsopimuksessa mainittuja tietoturvakäytäntöjä. Viestintäviraston (2015) mukaan etätyötä tekevän työntekijän tulisi pitää huoli seuraavista seitsemästä asiasta:

1. **Tietokoneen päivitys**. Päivitysten lataus ja asennus voidaan automatisoida yrityksen puolelta, mutta tietyissä tilanteissa ne vaativat käyttäjältä interaktiota, kuten päivitysten hyväksymistä tai uudelleenkäynnistystä. Näitä ei tulisi viivästyttää.
2. **Suojattujen verkkojen käyttö**. Julkisia WLAN eli langattomia lähiverkkoja tulisi välttää ja suosia esimerkiksi puhelimesta jaettua verkkoyhteyttä tuntemattomien verkkojen sijaan.
3. **Kotiverkon turvallisuus**. Vähintään mahdollinen tukiaseman oletuskäyttäjätunnus tulisi vaihtaa.
4. **Työtietokoneen käyttö**. Työtietokonetta tulee käyttää vain omassa käytössä. Näin vältyt muiden ihmisten aiheuttamilta vahingoilta, jotka saattavat useimmiten olla täysin tahattomia.
5. **Työnantajalta saatujen laitteiden käyttö**. Jos olet saanut työnantajan toimesta työvälineitä tai -laitteita, on suotavaa, että käytät niitä työnteossa. Tämän avulla voit olla varma, että tietokone on suojattu ainakin järjestelmien puolesta työnantajalle kelpaavalla tavalla.
6. **Työvälineistä huolehtiminen**. Työvälineitä ei tulisi jättää valvomatta missään olosuhteissa.
7. **Ammatillinen työasioiden hoito**. Älä puhu työasioista paikoissa, joissa ulkopuoliset saattavat niitä kuulla.

Nämä seitsemän kohtaa tuovat esille myös tietoturva fyysisen aspektin. Tietoturvallisuus ei ole aina näkymätön uhka vaan myös varkaudet ja tavaroiden kadottaminen asettavat arkaluontoiset tiedot vaaraan. Tästä syystä joissakin yrityksissä on etätyöskentelyyn liittyviä sääntöjä, jotka kieltävät muun muassa paperisten asiakirjojen ja muistiinpanojen viemisen pois työpaikalta. Myös mahdolliset kotona säilytettävät työvälineet tulisi pitää lukkojen takana, kun niitä ei käytetä. (Ervasti 2016.) Varkaudet ja tavaroiden kadottamisen todennäköisyys kasvaa etätyössä. Tämän johdosta yritykset saattavat vaatia heidän laitteisiin mahdollisuutta tyhjentää niiden muisti etäyhteyden avulla. (Viestintävirasto 2015.)

4 Etätyöskentelymenetelmät

Etätyön yleistymisen ja uudenlaisten teknologioiden myötä erilaisia etätyöhön soveltuvia menetelmiä on ilmestynyt markkinoille tasaisella tahdilla. Työn luonteen muuttuminen on pakottanut sovelluskehittäjät miettimään ratkaisuja, jotka tarjoavat niin työnantajalle kuin työntekijälle mahdollisimman otollisen ja ennen kaikkea vaivattoman tavan tehdä töitä etänä. (VAHTI 2009.)

4.1 VPN

VPN (Virtual private network) eli virtuaalinen erillisverkko tarjoaa käyttäjälle mahdollisuuden suojattuun yhteyteen oman organisaation lähiverkkoon tai tavan yhdistää yrityksen verkot toisiinsa. Sen alkuperäinen idea oli tarjota keino yhdistää maantieteellisesti eri sijainneissa sijaitsevia yrityksen toimipaikkoja toisiinsa, mutta on sittemmin vakiinnuttanut paikkansa muun muassa yksittäisten henkilöiden verkkoliikenteen salauksen työkaluna. Se suojaa yksittäistä käyttäjää Internet-palveluntarjoajien (ISP) sekä verkkosivustojen tarkkailulta ja poistaa eston hyödyntää maantieteellisesti rajattujen palveluiden käytön. (Viljanen 2016.)

Ilman VPN-yhteyttä käyttäjä ottaa ensin yhteyttä palveluntarjoajaan, joka yhdistää hänet haluamalleen sivustolle. Tällöin siis kaikki käyttäjän data kulkee Internet-palveluntarjoajan kautta, joka pystyy halutessaan tarkkailemaan heidän järjestelmiensä läpi kulkevaa tietoa. VPN-yhteyden kanssa käyttäjä yhdistää itsensä Internet-palveluntarjoajan sijaan ensin erilliselle VPN-palvelimelle, jota ylläpitää käyttäjän valitsema VPN-palveluntarjoaja. Tämä yhteys on salattu ja sitä kutsutaan myös VPN-tunneliksi. Tällöin Internet-palveluntarjoaja näkee ainoastaan sen, että käyttäjä on yhteydessä VPN-palvelimeen. (Crawford 2016.) Tähän salaukseen käytetään erityisiä avaimia, jotka ovat vain käyttäjän ja VPN-palveluntarjoajan tiedossa, mikä mahdollistaa sen, että tietoliikenne pystyy kulkemaan täysin salattuna (Vänskä 2015).

VPN-yhteyden turvallisuuteen vaikuttaa oleellisesti siinä käytetty protokolla. Käytetyimmät sekä yleisimmät protokollat ovat Crawfordin (2014) mukaan:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP) and Internet Protocol Security (IPSec)
- OpenVPN
- Secure Socket Tunneling Protocol (SSTP)
- Internet Key Exchange version 2 (IKEv2)

Näiden protokollien tärkeimpiä elementtejä on vertailtu tarkemmin alla olevassa taulukossa (taulukko 3).

Taulukko 3. VPN-protokollien vertailu (VPN University 2016)

	PPTP	L2TP/IPSec	OpenVPN	SSTP	IKEv2
Suojauksen taso	128-bit	256-bit	256-bit	256-bit	256-bit
Tuetut laitteistot	PC, Mac, Linux, iPhone, Android, osa reitittimistä	PC, Mac, Linux, iPhone, Android, osa reitittimistä	Lähes kaikki alustat, mutta vaatii ohjelmiston tuekseen, osa reitittimistä	Vain Windows PC:t	PC, Mac, Android, iPhone
Turvallisuus	Heikko	Vahva	Erittäin vahva	Vahva	Erittäin vahva
Nopeus	Erittäin nopea (heikon suojauksen johdosta)	Kohtalainen	Erittäin nopea	Kohtalainen	Erittäin nopea

Protokolla tulee valita omiin tarpeisiin sopivaksi. PPTP:tä pidetään yleisesti näistä vaihtoehdoista turvallisuudeltaan heikoimpana. Se kuitenkin paikkaa tätä puutetta nopeudellaan, minkä johdosta se soveltuu esimerkiksi maantieteellisesti suojattujen videoiden katseluun. OpenVPN puolestaan nostetaan useissa lähteissä parhaimmaksi protokollaksi turvallisuutensa ja nopeutensa ansioista, mutta haastava ympäristön pystytys ja tarve hankkia kolmannen osapuolen sovellus pakottavat käyttäjän harkitsemaan myös tämän vaihtoehdon hankintaa. Kaiken kaikkiaan OpenVPN on näistä vaihtoehdoista parhain sen nopeuden, turvallisuuden ja laitetuen osalta. (VPN University 2016.)

Vaikka VPN-yhteyttä voidaan käyttää useisiin eri käyttötarkoituksiin, on etätyöskentelyn kannalta sen tärkein ominaisuus kuitenkin mahdollisuus yhdistää itsensä yrityksen lähiverkkoon turvallisesti, sijainnista riippumatta. Tämä vaatii yleensä erillisen ohjelman asentamista käyttäjän koneelle. Tämä ohjelma vastaa tietosisällön salauksesta ja sen lähettämisestä oikeaan kohteeseen eli etätyöskenneltäessä yrityksen lähiverkkoon. Kohteessa VPN-palvelin vastaanottaa nämä sovelluksen salaamat paketit, purkaa ne ja lähettää puretut paketit eteenpäin oikeaan kohteeseen yrityksen lähiverkossa. Palvelin on myös vastuussa käyttäjän autentikoinnista. (Torres 2016.)

4.2 Työpöytävirtualisointi

Työpöytävirtualisoinnin ideana on irrottaa tietokoneen työpöytäympäristö eli käyttöjärjestelmä, käyttäjän henkilökohtaiset tiedostot sekä sovellukset fyysisestä tietokoneesta. Sovellusvirtualisointi puolestaan on virtualisoinnin muoto, jossa sovellus erotetaan käyttöjärjestelmästä, jolloin se voidaan toimittaa itsenäisenä komponenttina käyttäjän koneelle, joko etänä tai suoratoistolla. (Rouse 2016.) Vaikka työpöytävirtualisointi ja sovellusvirtualisointi ovat kumpikin omia virtualisoinnin muotoja, käytetään näitä kahta virtualisoinnin muotoa usein yhdessä. Työpöytävirtualisoinnissa käyttäjä ei aja yllä mainittuja komponentteja omalla koneellaan vaan ne pyörivät etäpalvelimella. Käyttäjä ottaa yhteyttä palvelimeen verkon yli ja työpöytä välitetään käyttäjälle välityspalvelimen (broker) avulla. (Beal.)

Koska käyttäjä tarvitsee vain verkkoyhteyden ja yleensä myös kolmannen osapuolen sovelluksen päästäkseen käsiksi omaan työpöytäänsä, tarjoaa työpöytävirtualisointi monia etuja etätyöskentelyn näkökulmasta. Käyttäjä saa tiedostot ja sovellukset käsiinsä mistä vain ja millä tahansa laitteella. (Beal.) Koska käyttöjärjestelmä, kaikkine komponentteineen, ei pyöri käyttäjän koneella vaan ainoastaan peilautuu sille, on työpöytävirtualisoinnissa mahdollista hyödyntää hieman heikompiakin laitteita, kuten esimerkiksi tabletteja tai thin clientteja. Thin clientit ovat niin sanottuja riisuttuja versioita normaaleista tietokoneista eli niiden fyysiset komponentit eivät ole yhtä tehokkaita kuin normaalin tietokoneen. (Madden 2011.) Tämä mahdollistaa myös freelancereille helpon tavan työskennellä. Sen sijaan, että yritys joutuisi asentamaan jokaiselle freelancerille oman koneen tai ohjaamaan häntä oman laitteen tietoturvan ja sovellusten kanssa, voi yritys asentaa hänelle työpöytävirtualisointiin käytettävän sovelluksen. Tällöin työntekijällä on valmis, yrityksen standardit täyttävä, työympäristö käytössään.

Työpöytävirtualisoinnissa käyttäjän data ei ole tallennettuna käyttäjän käyttämälle koneelle vaan se on säilössä palvelimella. Tämän pienentää esimerkiksi varkauksista koituvia tietoturvariskejä, koska laitteen hävitessä, se ei sisällä mitään tärkeää dataa. Myös mahdolliset laitteiden rikkoutumiset ja sitä kautta tiedostojen katoamiset voidaan ehkäistä, kun tieto on tallennettuna jossakin muualla. Kahdentamalla tallennettu data usealle eri palvelimelle voidaan myös ehkäistä käytettävyysongelmia. Tällöin toisen palvelimen hajotessa, käyttäjä pääsee automaattisesti hyödyntämään toisella palvelimella olevia tiedostoja, eikä se häiritse työntekoa. (McCabe 2010.)

4.3 Pilvipalvelut osana etätyöskentelyä

Pilvipalvelut voidaan määritellä palveluiksi, jotka tarjotaan ja joita hyödynnetään verkon yli. Käytännössä tämä siis tarkoittaa, että käyttäjän ei tarvitse ladata esimerkiksi ohjelmistoja omalle koneelleen tai tallentaa tiedostoja oman koneen kiintolevylle. Sen sijaan näitä sovelluksia ja tiedostoja voi hyödyntää ja selata verkkopohjaisilta alustoilta, jotka tarvitsevat toimiakseen ainoastaan verkkoyhteyden. (Rouse 2011.)

Tarjolle on ilmestynyt lähihistoriassa myös kokonaisia paketteja, jotka sisältävät tiedostontallennuksen lisäksi muun muassa tekstinkäsittelyohjelman, viestintä- sekä sähköpostisovelluksen. Kaikki nämä ovat käyttäjälle tarjolla, kunhan hänellä on toimiva verkkoyhteys. Käyttäjän ei tarvitse halutessaan ladata koneelleen yhtäkään sovellusta tehdäkseen työnsä. Tämänkaltainen ratkaisu on oiva tapa mahdollistaa etätyöskentely sijainnista ja laitteesta riippumatta. Tällä hetkellä kaksi suosituinta pilvipohjaista sovelluskokonaisuutta ovat **Microsoft Office 365** ja **Google Apps for Work**. Tästä syystä juuri nämä kaksi vaihtoehtoa valittiin vertailuun. Vertailun osa-alueet valittiin niiden oleellisuuden takia, joista esimerkiksi hinta ja pakettiin sisältyvät sovellukset ovat hyvin tärkeitä elementtejä kokonaisuuden kannalta. Tarkempi vertailu näiden kahden sovelluksen ydinkomponenteista löytyy taulukosta 4. Vaikka Google tarjoaa hyvän vaihtoehdon Microsoftin Office 365 korvaajaksi, jää se silti tietyissä asioissa jälkeen, kuten yhteensopivuudessa ja sovellusten hyödyllisissä ominaisuuksissa. Tästä syystä se on hyvä vaihtoehto pienille ja aloitteleville yrityksille, mutta suurempien organisaatioiden käytössä sen toiminnallisuudet eivät riitä takaamaan riittävän tehokasta ja vaivatonta työskentelyä. (Kapko 2015.)

Taulukko 4. Google for Work vs Office 365 (Kapko 2015)

	Google for Work	Office 365
Aloitusmaksu	$5/kk tai $50/vuosi	$5/kk per käyttäjä vuoden sitoutumisella
Tallennustila	30 GB/käyttäjä, rajoittamaton premiumkäyttäjille joilla vähintää viisi käyttäjää	1 TB
Lisenssivaihtoehdot	$5 tai $10	$5, $8,25 tai $12,50/käyttäjä business käyttäjille; $8, $12, $20 enterprise käyttäjille
Sovellukset	Gmail, Hangouts, Drive ja Docs	Word, Excel, Outlook ja PowerPoint
Sitoutuminen	Kuukausittainen tai alennettuna koko vuosi	Vuosittainen

Tietoturvanäkökulmasta katsottuna kumpaakin ratkaisua voidaan pitää turvallisena. Molemmat säilövät tallennetut tiedot tarkkaan suojattuihin datakeskuksiin, joiden tietoturva on epäilemättä paremmalla tasolla, kuin yksittäisen käyttäjän. Google lupaa käyttöehdoissaan, että se ei käytä Driveen eli tiedostonhallintasovellukseen tallennettuja tiedostoja markkinointitarkoituksiin. Molempien kokonaisuuksien kohdalla harmittavaa on se, että esimerkiksi salasanavuoden sattuessa avautuu pääsy käyttäjän tiedostojen lisäksi myös sähköpostiin. Molemmat tarjoavat myös usean asteen tunnistuksen, joka tarkoittaa käyttäjätilin suojausta salasanan lisäksi esimerkiksi puhelimeen lähetettävällä koodilla (Smith 2014.)

5 Etätyömenetelmien tietoturva

Tutkimuksen tavoitteena oli selvittää eri etätyömenetelmien tietoturvan taso. Tämä raportti sisältää kolmen eri etätyömenetelmän testauksen ja niiden analysoinnin tietoturvan tavoitteiden kannalta. Tutkimukseen valikoituivat seuraavat etätyömenetelmät:

- VPN-yhteys
- Työpöytävirtualisointi
- Pilvipavelut osana etätyöskentelyä

Huomion arvoista on, että kaikkien näiden menetelmien konfiguraatioita, kuten esimerkiksi autentikointia, voidaan muokata omaan yritykseen sopivaksi. Tämä onnistuu lisäämällä tai vähentämällä autentikointivaiheessa kysyttyjä tunnistautumistietoja. Tämän lisäksi käytettäviä ohjelmistoja on useita ja niiden toiminta saattaa poiketa tässä tutkimuksessa käytettävistä ohjelmista tiettyjen vaiheiden osalta.

Eri etätyön menetelmiä lähdettiin tutkimaan hyvin käytännönläheisesti hyödyntämällä kullekin menetelmälle räätälöityä ohjelmistoa. Tarkoituksena oli pyrkiä pääsemään käsiksi yrityksen sisäiseen, jaettuun tiedostoon, muokkaamaan sitä ja tallentamaan muutokset. Samassa yhteydessä kerrottiin, kuinka nämä vaiheet toteuttavat tietoturvalle asetettuja tavoitteita. Testauksen kautta pyrittiin havaitsemaan mahdolliset aukot tai puutteet tietoturvassa ja tätä kautta kehittämään ratkaisuja, joiden avulla esille nousseet tietoturvariskit voidaan minimoida. Tämän kaltaisen lähestymistavan ansiosta saadaan käsitys siitä, miltä menetelmän hyödyntäminen näyttää loppukäyttäjän näkökulmasta.

5.1 VPN-yhteyden tietoturva

VPN-yhteyden testaamiseen käytettiin SonicWALLin tarjoamaa ohjelmistoa nimeltä SonicWALL Global VPN Client. Ohjelmiston ideana on luoda turvallinen ja salattu VPN-tunneli pääkäyttäjän laitteen ja yrityksen lähiverkon välille.

Kuten monet muutkin VPN-yhteydellä toteutettavat yhteydet, joissa yksittäinen käyttäjä ottaa yhteyttä yrityksen lähiverkkoon, myös SonicWALL tarvitsee tuekseen pääkäyttäjän koneelle asennettavan ohjelmiston. Ohjelmiston asennuksen jälkeen se konfiguroitiin siten, että sovellus osaa ottaa yhteyttä oikeaan palvelimeen eli sille syötettiin oikea porttikäytävä (gateway). Sovelluksen konfigurointi ei vaadi pääkäyttäjältä tämän lisäksi muita tietoja osatakseen ottaa yhteyttä oikeaan palvelimeen. Käyttäjän käyttökokemuksen parantamiseksi sovellus määriteltiin vielä ajamaan käyttäjän sisäänkirjautumisskripti yhteyden muodostuksen jälkeen. Tämän avulla esimerkiksi käyttäjän verkkoasemat saadaan ilmestymään automaattisesti resurssienhallintaan, mikä helpottaa tiedostoihin käsiksi pääsemistä.

Kun uusi yhteys oli luotu, se tuli käynnistää. Ensimmäinen vaihe yhteyden luonnissa oli ISAKMP eli Internet Security Association and Key Management Protocol, jonka tarkoituksena on sopia osapuolten kesken, kuinka salaukseen käytettäviä avaimia vaihdetaan. Protokolla itsessään ei siis hoida avaimien vaihtoa vaan tarjoaa ainoastaan viitekehyksen sille, kuinka avainten vaihto tapahtuu.

Tämän jälkeen IKE eli Internet Key Exchange hoiti annetun viitekehyksen avulla yhteyden muodostamisen ja turvasi täten tiedon lähetyksen ja vastaanoton. Nämä vaiheet eivät näkyneet käyttäjälle, ellei hän niitä sovelluksen lokitiedoista käy katsomassa tai seuraa tarkasti sovellusikkunaa, jossa yhteyden tila muuttuu ensimmäisen vaiheen jälkeen muotoon "Connected" ja toisen vaiheen jälkeen yhteyden eteen ilmestyy vihreä oikein-merkki.

Nämä vaiheet näkyivät pääkäyttäjälle selkeimmin jaetun salaisuuden (Pre-Shared Key) kyselynä. Global VPN Client tukee kahta eri IPSecin autentikointimenetelmää, jotka ovat **jaettu salaisuus** ja **kolmanten osapuolten sertifikaatit**. Tässä tapauksessa autentikointi oli määritelty tapahtumaan jaetun salaisuuden avulla, joka on näistä kahdesta vaihtoehdosta yleisemmin käytetty IPSecin autentikointimentelmä. Jaettu salaisuus on etukäteen määritelty 4-128 merkkiä pitkä salasana, jota VPN-tunnelin eri päätepisteet käyttävät määritelläkseen tiedon turvallisen siirron protokollista. Jaettu salaisuus voidaan myös määritellä osaksi yhteyttä, jolloin se toimitetaan esimerkiksi asennuspaketin mukana. Tässä tapauksessa jaettu salaisuus oli kuitenkin ilmoitettu järjestelmänvalvojan toimesta ja se tuli syöttää kysyttäessä. Kolmanten osapuolten sertifikaatteja tulisi hallinnoida Certificate Managerilla, jonka avulla Global VPN Clienttia ohjeistettaisiin käyttämään digitaalisia sertifikaatteja. Tämä vaatii enemmän osaamista ja työtä, minkä takia jaetut salaisuudet ovat suositumpi vaihtoehto.

Seuraavassa vaiheessa käyttäjä tunnistettiin käyttäjätunnuksen ja salasanan avulla. Tunnistus voi tapahtua joko SonicWALLin tietokannan avulla, RADIUS palvelimen avulla tai näiden kahden menetelmän yhdistelmällä. Ikkunaan syötettiin käyttäjänimi muodossa toimialue\käyttäjänimi ja käyttäjän toimialueen käyttäjätunnuksen salasana. Annettu tunnus tarkastettiin edellä valitun menetelmän avulla validiksi ja yhteys muodostettiin onnistuneesti.

Kun yhteys oli muodostettu onnistuneesti, oli käyttäjällä pääsy lähiverkossa sijaitseviin kansioihin. Kansiot oli jaettu yrityksen tiedostopalvelimella ja oikeudet näihin kansioihin oli määritelty sitä kautta. Tiedostopalvelinta on mahdollista ylläpitää joko yrityksen omissa tiloissa tai siirtää palvelimet pilveen virtuaalipalvelimiksi, jolloin niiden toiminnallisuudesta vastaa kolmas osapuoli, mutta sisältö luodaan itse. Tässä tapauksessa tiedostopalvelin oli

virtualisoituna pilvessä. Käyttäjän oikeudet näihin kansioihin olivat täysin samat kuin lähiverkossa. Jotta tiedostoa pystyttiin muokkaamaan, tuli käytettävällä koneella olla tiedoston muokkaamiseen soveltuva ohjelma.

Näitä VPN-yhteyden vaiheita, aina sen muodostamisesta, tiedoston muokkaukseen ja sen tallennukseen, lähdettiin vertaamaan tietoturvan tavoitteisiin, jotka on käyty läpi kappaleessa 2.3.2. Alla oleva taulukko (taulukko 5) käsittelee näitä kuutta tietoturvan tavoitetta ja sitä, miten ne on VPN-yhteydessä toteutettu.

Taulukko 5. VPN-yhteyden tietoturva

VPN-yhteyden tietoturva

Luottamuksellisuus	VPN-yhteys todentaa käyttäjän kahteen kertaan jaetun salaisuuden ja käyttäjätunnuksen avulla. Palvelimella sijaitseviin tiedostoihin on myönnetty pääsyoikeus vain tietyille henkilöille.
Eheys	VPN-tunneli takaa turvallisen tiedonsiirron käyttämällä IPSec salaustekniikkaa.
Saatavuus	Käyttäjän oikeudet muodostaa VPN-yhteys sekä oikeudet lukea ja muokata tiedostoja palvelimella, määritellään käyttäjätilin luonnin yhteydessä. Palvelinten toiminnallisuudesta vastaa kolmas osapuoli, jonka tehtävänä on pitää ne toimintakunnossa.
Todentaminen	Todentaminen tapahtuu kahdessa eri vaiheessa. Ensimmäisessä vaiheessa käyttäjä syöttää yrityksen sisäisesti jaetun salasanan (Pre-Shared Key). Toisessa vaiheessa käyttäjä syöttää käyttäjätunnuksen sekä salasanan, jonka avulla hän todistaa olevansa käyttäjätilin omistaja.
Pääsynvalvonta	Toteutetaan jaetulla salaisuudella sekä käyttäjätunnuksen sekä salasanan yhdistelmällä.
Kiistämättömyys	VPN-tunnelin muodostuksen yhteydessä molemmat osapuolet todistavat olevansa, keitä he väittävät olevansa.

5.2 Työpöytävirtualisoinnin tietoturva

Työpöytävirtualisoinnin testaus toteutettiin Citrixin tuotteilla. Apuna käytettiin Citrix Receiveriä, jonka tarkoituksena oli hoitaa liikennöinti päätelaitteen ja VDI-palvelimen välillä. Tämä sovellus mahdollistaa työpöytävirtualisoinnin käytön, joka puolestaan oli toteutettu Citrixin XenDesktopilla. Pääkäyttäjän koneelle tuli siis ladata Citrix Receiver, jotta päästiin alkuun. Sovellus on maksuton, eikä sen lataukseen tarvita lisenssejä. Tämän lisäksi huomionarvoista on se, että sovelluksen pystyy ladata melkeinpä mille tahansa päätelaitteelle, mikä mahdollistaa oman työpöydän käytön jopa älypuhelimelta.

Sovelluksen latauksen jälkeen tuli ohjelmaan määritellä uusi käyttäjä ja tässä tapauksessa siinä hyödynnettiin käyttäjän tunnusta omalle toimialueelleen. Tämän enempää määrittelyjä sovelluksen toiminta ei vaatinut vaan se oli käyttövalmis. Jotta omaa virtuaalityöpöytää päästiin käyttämään, tuli seuraavaksi kirjautua sisään. Sisäänkirjautuminen onnistui joko verkon kautta, yrityksen omaa URL-osoitetta käyttäen, tai suoraan sovelluksesta käsin. Selaimella kirjauduttaessa sivusto on https-suojattu TLS-salauksella, jonka tarkoituksena on mahdollistaa tiedon kuljettaminen eheästi ja salatusti kahden sovelluksen välillä.

Ensimmäisessä vaiheessa käyttäjä tunnistetaan kahdella eri koodilla. Toinen näistä oli yritykseltä saatu henkilökohtainen pin-koodi ja toinen oli käyttäjän oma salasana. Käyttäjätunnuksena toimi tässä tilanteessa sama tunnus, jolla hänet normaalisti tunnistettaisiin yrityksen lähiverkossa. Kun kaikki kolme tunnusta oli syötetty onnistuneesti, päästi sovellus kirjautumaan sisään. Tässä vaiheessa on mahdollista antaa käyttäjälle valinta valita hänelle osoitetuista työpöydistä haluamansa tai ohjata hänet tiettyyn työpöytään. Koska tässä tapauksessa työpöytä oli määritelty käyttäjälle yrityksen puolesta, ei tätä valintaa tullut vaan käyttäjä ohjautui suoraan omalle työpöydälleen.

Työpöytä siis sijaitsee virtuaalipalvelimella, josta käyttäjän työpöytä ainoastaan ohjataan näkymään hänen käyttämälleen päätelaitteelle. Tästä syystä tietyt komponentit eivät ole normaalin työaseman tapaan käytettävissä. Esimerkiksi verkkosijainnit ja ulkoiset tallennusvälineet saadaan näkymään käyttäjälle ja hän pystyy hyödyntämään niitä normaalisti eli tallentamaan ja lukemaan muun muassa tiedostoja niiltä. Se, millaisen työpöydän käyttäjä saa käyttöönsä, on yrityksen päätettävissä ja sen sisältämät komponentit, kuten sovellukset ja verkkolevyt, voidaan määritellä tapauskohtaisesti.

Ideana oli päästä muokkaamaan yrityksen lähiverkossa sijaitsevaa tiedostoa. Virtuaalityöpöytä sisälsi tähän tarvittavat ohjelmat, joten erillisiä sovelluksia ei tarvinnut ladata omalle koneelleen alussa asennettua Citrix Receiveriä lukuun ottamatta. Koska verkkosijainnit oli

määritelty näkymään automaattisesti, onnistui niihin käsiksi pääsy ilman sen suurempia ongelmia tai määrittelyjä. Virtuaalityöasemat oli määritelty vaihtumaan joka kirjautumiskerran yhteydessä, minkä johdosta tiedoston tallennus tuli tehdä sijaintiin, joka uuden kirjautumiskerran yhteydessä on jälleen käyttäjän saatavilla. Tähän soveltui mainiosti verkkoasema, jonka sisältö oli tallessa konesaleissa. Esimerkiksi koneen paikalliselle kiintolevylle tehdyt tallennukset eivät olisi enää näkyneet seuraavan kirjautumisen yhteydessä. Tiedosto saatiin onnistuneesti muokattua ja tallennettua. Jotta varmistuttiin, että kaikki tämä tapahtui onnistuneesti, kirjauduttiin työpöydältä kerran ulos ja takaisin sisään, jonka jälkeen muokatun tiedoston havaittiin olevan oikeassa muodossa myös uudelle kirjautumisen jälkeen.

Myös työpöytävirtualisoinnin eri vaiheita lähdettiin analysoimaan tietoturvalle asetettujen tavoitteiden kautta. Alla olevassa taulukossa (taulukko 6) on kuvattu sitä, kuinka ne on täytetty.

Taulukko 6. Työpöytävirtualisoinnin tietoturva

Työpöytävirtualisoinnin tietoturva

Luottamuksellisuus	Työpöytävirtualisointi edellyttää käyttäjän tunnistautumista omalla käyttäjätunnuksellaan. Ulkopuoliset eivät pysty kirjautumaan käyttäjän koneelle ilman näitä tunnuksia. Tiedostot säilytetään palveluntarjoajan palvelimilla konesaleissa.
Eheys	Dataa ei siirretä palvelimen ja käyttäjän päätelaitteen välillä vaan se sijaitsee jatkuvasti palvelimella. Ainoastaan käyttäjän hiiren ja näppäimistö painallukset siirtyvät verkon yli. Palvelimen ylläpitäjä on vastuussa tiedon säilömisestä.
Saatavuus	Palvelimia, joissa käyttäjien virtuaalityöpöydät ja data sijaitsevat on yleensä vähintään kaksi, jolloin toisen kaatuessa, käyttäjät ohjataan toissijaiselle palvelimelle. Kirjautuminen onnistuu selaimen tai sovelluksen kautta, mikä tarjoaa useamman pääsykanavan.
Todentaminen	Käyttäjä todennetaan käyttäjätunnuksella ja salasanalla sekä mahdollisesti yrityksen sisäisellä pin-koodilla, joka on henkilökohtainen.
Pääsynvalvonta	Päästäkseen työpöytäänsä käsiksi, käyttäjän tulee antaa pääsyyn oikeuttava käyttätunnuksen ja salasanan yhdistelmä sekä mahdollinen pin-koodi. Pääsynvalvontaa voidaan myös parantaa sirukorteilla tai muilla vastaavilla tuotteilla.
Kiistämättömyys	Virtuaalityöpöytien transaktio lokit sisältävät yleensä tiedon siitä, kuka konetta on käyttänyt ja mikä virtuaalikone istuntoa on hoitanut.

5.3 Pilvipalveluiden tietoturva

Pilvipalveluiden hyödyntämistä osana etätyöskentelyä lähdettiin testaamaan Microsoftin Office 365 palvelulla. Tämän pilvipalvelun ideana on tarjota yritykselle yksinkertainen hallinta-alusta niin käyttäjätunnuksille kuin esimerkiksi sähköpostilaatikoiden hallinnalle. Paketti on hyvin mukautuva ja sitä voidaan käyttää yrityksen tarpeisiin heidän haluamallaan tavalla, joko lisäten tai karsien tiettyjä elementtejä. Yksittäisen käyttäjän ja varsinkin etätyötä tekevän työntekijän kannalta tämän pilvipalvelun tärkeimpiä ominaisuuksia ovat kuitenkin verkon yli käytettävät sovellukset. Näihin sovelluksiin kuuluvat mm. Word, Excel ja PowerPoint sekä OneDrive. Näistä sovelluksista OneDrive on oiva tapa säilöä dokumentteja siten, että ne ovat työntekijän käytettävissä missä tahansa verkkoyhteyden omaavassa paikassa. Palvelu on käyttäjälle maksullinen ja sen hintaa on selvitetty yrityskäytössä taulukossa 4. Myös yksittäinen henkilö voi hyödyntää Office 365 tarjoamia palveluita hintaan 70–90$ vuodessa riippuen paketista.

Etätyöntekijän näkökulmasta asiaa lähdettiin kuitenkin testaamaan yrityskäytössä olevalla Office 365 lisenssillä. Sovellukseen kirjaudutaan selaimen kautta ja kirjautumissivusto on suojattu https-salauksella TLS:n avulla. Kirjautumissivustolla kysyttiin käyttäjätunnusta ja salasanaa. Käyttäjänimi-kenttään syötettiin käyttäjän yrityksen alainen sähköpostiosoite. Tämän jälkeen sivusto ohjautui automaattisesti yrityksen omalla autentikointisivustolle. Tähän avautuneeseen ikkunaan syötettiin jälleen käyttäjätunnus ja käyttäjän salasana omalle toimialueelleen. Kun tunnistautuminen oli tapahtunut onnistuneesti, myönnettiin käyttäjälle pääsy oman Office 365:n aloitussivustolle.

Office 365:een kuuluva sovellus nimeltä OneDrive toimii pilvitallennustilana. Tämä siis mahdollistaa tiedoston käsittelyn eli lukemisen ja muokkaamisen, kunhan käyttäjä kirjautuu onnistuneesti sisään. Office 365 siis ei tarjoa käyttäjälle mahdollisuutta päästä yrityksen lähiverkkoon, joten kaikki siellä sijaitsevat tiedostot ovat tällä menetelmällä käyttäjän tavoittamattomissa. Tiedostot, joita halutaan OneDriven kautta jakaa, tulee siis myös tallentaa sinne, eikä niitä voi säilöä esimerkiksi oman yrityksen verkkosijainteihin. Kun tiedosto on ladattu OneDriveen, on sitä mahdollista jakaa haluttujen käyttäjien kanssa hyvin yksinkertaisesti, muutamalla painalluksella. Oletusarvona yksikään käyttäjän lataamista tiedostoista ei ole jaettu, ellei sitä ole tallennettu kansioon, joka on. Jotta tiedostojen lataus olisi mahdollisimman yksinkertaista, on käyttäjän mahdollista ladata OneDrive sovellus omalle koneelleen, jonka avulla kaikkia siellä olevia tiedostoja pystytään muokkaamaan myös suoraan tietokoneen resurssienhallinnasta. Tämä helpottaa työskentelyä siinä

määrin, että tiedostoja muokatakseen, käyttäjän ei aina tarvitse kirjautua sisään selaimen kautta.

Tästä lähdettiin navigoimaan käyttöliittymän kautta ensin OneDrive sovellukseen ja siitä oikeaan tiedostosijaintiin. Tässä tapauksessa tiedosto oli jaettu käyttäjän kanssa ja hänelle oli myönnetty siihen täydet luku- ja kirjoitusoikeudet. Tiedostoa pystyttiin muokkaamaan joko selaimessa niin sanotulla online-versiolla tai käyttäjän koneella olevalla sovelluksella. Online-versio on hieman karsitumpi, eikä se välttämättä tue uusimpia tiedostomuotoja, joten parhaan mahdollisen käyttökokemuksen turvaamiseksi, tiedostoa muokattiin koneella olevalla sovelluksella. Huomioitavaa kuitenkin on, että halutessaan käyttäjää ei velvoiteta lataamaan sovelluksia omalle koneelleen. Tiedostoa muokattaessa, aina tallennuksen yhteydessä, uusin versio lähetetään välittömästi myös palvelimelle. Kun tiedostoa oli onnistuttu muokkaamaan, se tallennettiin ja sovellus suljettiin. Muokkauksen onnistuminen tarkastettiin kirjautumalla Office 365 toiselta koneelta, jolta samaisen tiedoston sisältö todettiin muokatuksi.

Taulukossa 7 on esitelty, kuinka Office 365 pilvipalvelu täyttää tietoturvalle asetetut tavoitteet.

Taulukko 7. Pilvipalvelu Office 365:n tietoturva

Pilvipalvelun tietoturva

Luottamuksellisuus	Käyttäjä tunnistetaan SSL/TLS suojattujen sivustojen kautta ja myös kaksivaihenen tunnistaminen on mahdollista. Tiedot sijaitsevat palvelinsaleissa, jotka on suojattu useilla eri tasoilla.
Eheys	Käyttäjän data salataan palvelimilla sekä levyn suojauksella, että tiedoston suojauksella.Siirettäessä käytetään mm. TLS:ää ja IPseciä.
Saatavuus	Dataa säilötään useissa eri maantieteellisissä sijainneissa ja niitä varmuuskopioidaan sekä säilössä, että siirettäessä. Tunnistautumista hoitavat useat palvelimet. Virhetilanteessa automaattinen vianhallinta ohjaa käyttäjät toimiville palvelimille.
Todentaminen	Käyttäjä todennetaan käyttäjätunnuksen ja salasanan avulla, joka voidaan yhdistää yrityksen omaan AD:seen, jolloin vain yrityksen sallimilla henkilöillä on pääsyoikeus. Tarvittaessa todentamista voidaan parantaa lisäämällä kaksivaiheinen todentaminen.
Pääsynvalvonta	Käyttäjätunnukseksi kelpaa henkilön yrityksen alainen sähköpostiosoite ja oman toimialueen salasana.
Kiistämättömyys	Jokainen tiedosto salataan omalla avaimella, jonka vain käyttäjä voi avata.

5.4 Etätyömenetelmien riskit ja parannusehdotukset

Etätyön ja siihen käytettävien sovellusten ja menetelmien yleistyessä, on niiden tietoturvaan panostettava yhä enemmän. Suuremmat käyttäjäkunnat luovat houkutusta kaapata yrityksen kallisarvoisia ja arkaluontoisia tietoja. Vaikka menetelmiä onkin kehitetty kovaa tahtia, löytyy niistä silti myös heikkouksia ja haavoittuvuuksia. Yksikään menetelmä ei ole tietoturva-aukoton ja tästä syystä tärkeintä on pyrkiä pysymään kehityksen saralla haitta-ohjelmia edellä.

5.4.1 VPN-yhteyden haavoittuvuudet

Kuten muissakin etätyömenetelmissä, myös VPN:n yhteyksien suurin huolenaihe on pääkäyttäjien laitteet. VPN:n yhteyden perimmäinen tarkoitus on turvata käyttäjän ja yrityksen sisäisen lähiverkon liikenne. Tämä ei kuitenkaan takaa sitä, että tunnelin pääteasema eli tässä tapauksessa käyttäjän laite, olisi suojattu oikealla tavalla. Jos käyttäjän laite on altistunut esimerkiksi virukselle, avatessaan VPN-yhteyden, hän luo hakkerille suoran linjan yrityksen lähiverkkoon, jossa mahdolliset tuhot voivat olla hyvinkin mittavia.

BYOD eli bring your own device ratkaisun tarkoituksena on antaa käyttäjille mahdollisuus työskennellä hänen omalla laitteellaan. Idea tämän takana on hyvin yksinkertainen. Käyttäjän hyödyntäessä omaa laitettaan, työnantaja säästyy kustannuksilta, joita laitteiden hankkiminen tuottaa. Tällöin käyttäjä saa myös itse valita laitteensa omien mieltymysten mukaan. Tämä kuitenkin tuottaa suuria huolenaiheita erityisesti tietoturvaa silmällä pitäen. Koska käyttäjä itse on vastuussa laitteestaan, eikä työnantaja ole konfiguroinut sitä haluamallaan tavalla, voi sen virustorjunta ja muut tärkeät komponentit olla hyvinkin heikolla tasolla. Samainen ongelma ilmenee luonnollisesti julkisissa tietokoneissa, joiden käyttö työasioiden hoidossa tulisi ehdottomasti kieltää.

Jotta tämän kaltainen tilanne pystyttäisiin ennaltaehkäisemään, on työnantajan hankittava työntekijöilleen laitteet, jolloin niiden konfiguraatiot voidaan tehdä halutulla tavalla. Jos laitteita ei haluta hankkia, on työntekijöille vähintäänkin tarjottava kattava etätyöskentelyohjeistus ja mahdollisesti velvoitettava heitä asentamaan sovitut virustorjuntaohjelmat koneilleen. VPN-ohjelman tulisi myös suorittaa mahdollisten lokitietojen siivous käytetyltä koneelta. Täten estetään VPN-yhteyteen käytettyjen tietojen säilöminen koneelle, josta niiden saatetaan päästä käsiksi.

Julkiset verkot tarjoavat käyttäjille helpon ja mutkattoman tavan päästä verkkoon käsiksi, vaikka yleisessä kahvilassa. Niiden ongelma on kuitenkin tiedon puute siitä, kuinka ne on

turvattu. Kuten omien laitteiden käytössä, myös julkisten verkkojen hyödyntämisen suurin riski on siinä, ettei työnantaja pysty määrittelemään sille tarvittavia suojauksia. Julkiset yhteydet saattavat kuljettaa tietoa useiden eri tukiasemien kautta ja jos niiden suojaus ei ylety tarpeeksi syvälle tietoliikenteen salaamisen osalta, luo tämä riskin mahdollisille tietomurroille. Vaikka itse liikenne pystytään VPN:n avulla salaamaan, jos tunnelin päätepisteen tietoja saadaan selville, kuten esimerkiksi IP-osoite, voidaan pelkästään sillä saada tuhoa aikaan. Luonnollisesti helpoin tapa välttää tämän kaltaisia uhkia, on käyttää VPN:n yhteyttä ainoastaan silloin, kun ollaan verkossa, jonka tiedetään olevan turvallinen. Julkisia verkkoja tulisi välttää mahdollisimman paljon, jos niiden suojauksen tasosta ei ole tietoa. Suositeltavaa onkin esimerkiksi jakaa verkkoyhteys oman puhelimen avulla, jonka suojaustaso voidaan asettaa omien standardeiden mukaiseksi.

VPN-yhteyden konfiguraatioita muutetaan hyvin harvoin, koska tämä tuottaa lisää työtä niin yrityksen tietoturvasta vastaaville, kuin myös itse VPN-yhteyttä käyttäville työntekijöille. Tämä kuitenkin asettaa haasteita esimerkiksi työpaikasta lähtevien henkilöiden osalta. Työsuhteen päättyessä riitaisissa merkeissä, voi työntekijällä jäädä katkeria tunteita työnantajaansa kohtaan. Koska hänelle on aiemmin ollut tiedossa VPN-yhteyteen tarvittavat tiedot, ei kukaan saa häneltä näitä pois. Vaikka hyvin monet menetelmät käyttävät useita eri autentikointivaiheita, heikon käyttäjähallinnan ja pysyvien konfiguraatioiden johdosta, on lähteneellä työntekijälle silti erittäin paljon yhteyden luomiseen tarvittavia tietoja hallussaan. Käyttäjähallinta tulisi pitää sillä tasolla, että lähteneiden työntekijöiden tilit suljetaan viipymättä ja täten estetään käyttäjän pääsy tietovarastoihin heti lähdön jälkeen.

Koska esimerkiksi VPN-porttikäytävän uudelleenkonfigurointi on hyvin aikaa vievää ja tuottaa paljon työtä sen tekevälle henkilölle, on muita VPN-yhteyden komponentteja järkevämpää muokata. Esimerkiksi tässä testauksessa käytetyn Global VPN Clientin ominaisuuksiin kuuluu jaetun salaisuus, jota tulisi tasaisin väliajoin muokata. Vaihtoehtoisesti jaetun salaisuuden tilalla oleva sertifikaatti tulisi uusia tarpeen mukaan.

5.4.2 Työpöytävirtualisoinnin haavoittuvuudet

Työasemavirtualisoinnin suurin riski liittyy juuri sen helppoon käytettävyyteen. Koska työasemaan pääsee käsiksi mistä vaan, jossa on toimiva verkkoyhteys, on teoriassa kenellä tahansa mahdollisuus kirjautua sisään työntekijän koneelle. Laitteiden fyysiset varkauden ovat aina läsnä, kun käyttäjällä on tietokone mukanaan julkisella paikalla ja tietysti myös toimistolla. Jos vastakkain asetellaan fyysisen koneen varastaminen ja virtualisoidulle työpöydälle kirjautuminen, on näistä kahdesta jälkimmäinen huomattavasti helpompaa, mikäli käyttäjä ei ole tietoturva-asioiden kanssa valveutunut. Tietojen varastamista suunnittelevan henkilön täytyy virtualisoidun työpöydän kanssa selvittää työntekijän sisäänkirjautumistunnukset ja tietomurto voidaan tehdä vaikka omasta kodista käsin. Fyysisen tietokoneen varastaminen sen sijaan vaatii sekä itse laitteen anastamista että tietokoneen hakkerointia. Tämä estetään sillä, että virtuaalityöpöytään vaadittavat sisäänkirjautumismenetelmät asetetaan mahdollisimman monivaiheisiksi. Esimerkiksi kaksivaiheinen autentikointi auttaa asiaa. Lisäksi olisi syytä luoda käyttäjälle aina uusi sessio hänen kirjautuessaan sisään ja tällä tavalla poistaa edellisen istunnon jäljet koneelta.

Komponenttien säilöminen fyysisesti eri sijainteihin käyttäjien kanssa luo sekä mahdollisuuksia että riskejä. Pahimmassa tapauksessa palvelimet, jotka sisältävät käyttäjien koneet ja kaiken datan, saattavat tuhoutua tai vähintäänkin kokea hetkellisiä saatavuusongelmia esimerkiksi tulipalon, luonnonkatastrofin tai sähkökatkon johdosta. Luonnollisesti nämä samaiset riskit ovat olemassa, vaikka käyttäjällä olisikin normaali, eikä virtualisoitu työympäristö. Yleensä näissä tilanteissa säilyy kuitenkin vähintään toinen käyttäjän tarvitsemista laitteista, oma tietokone tai palvelimet.

Tämän kaltaisia tilanteita voidaan kuitenkin ehkäistä hajauttamalla palvelimia esimerkiksi maantieteellisesti eri sijainteihin ja peilata useita palvelimia toimimaan toistensa toissijaisina palvelimina. Tämä tarkoittaa käytännössä sitä, että jos käyttäjän käyttämä ensisijainen palvelin hajoaa, osataan hänet ohjata automaattisesti toissijaiselle palvelimelle, joka toimii täysin samalla tavalla. Käyttäjän näkökulmasta minkäänlaista ongelmaa ei ilmene. Yrityksen näkökulmasta kyseinen ongelma on tietysti haastava, koska palvelimien ylläpito on ulkoistettu, eikä niitä käyttävällä yrityksellä ole välttämättä mahdollisuutta vaikuttaa niiden toimintaan. Eri palveluntarjoajien kilpailutus kuitenkin on mahdollista ja valintaa tehdessä, on syytä kiinnittää huomiota esimerkiksi palvelimien sijainteihin ja niiden ominaisuuksiin.

Työpöytävirtualisointi nojaa myös hyvin vahvasti käytettävän verkkoyhteyden laatuun, koska käytännössä kaikki siirretään verkon ylitse, vaikka prosessit tapahtuvatkin palvelinsaleissa. Ilman toimivaa verkkoyhteyttä, työntekijä ei käytännössä pysty tekemään yhtään mitään, mikä vaarantaa erityisesti saatavuuden. Samainen ongelma ilmenee muissakin etätyöskentelymenetelmissä, koska ne kaikki vaativat toimiakseen verkkoyhteyttä. Muissa tämän raportin menetelmissä käyttäjällä on kuitenkin työvälineenään yleensä täysin normaali tietokone, eikä esimerkiksi thin client, joita työpöytävirtualisoinnissa voidaan hyödyntää. Thin clienteissa vianhallinta on vaikeampaa niiden riisutuiden ominaisuuksien johdosta. Tämän takia on ensisijaisen tärkeää, että yrityksen verkkoyhteys on sillä tasolla, että sen toimintaan voidaan luottaa.

Etätyöntekijä on vastuussa oman kotinsa verkkoyhteyden toimivuudesta. Verkkoyhteysongelmat ovat siinä mielessä haastavia, että ne liittyvät hyvin usein kolmanteen osapuoleen, joka tässä tapauksessa on palveluntarjoaja. Näiden kilpailuttaminen nopeimman verkkoyhteyden löytämiseksi on ensimmäinen askel onnistuneeseen ympäristöön. Reitittimet kannattaa kotioloissa asettaa mahdollisimman keskeiselle paikalle, jolloin varsinkin langatonta yhteyttä käytettäessä niiden signaali on vahvin mahdollinen. Suositeltavaa on käyttää langallista yhteyttä.

5.4.3 Pilvipalveluiden haavoittuvuudet

Suurin ja yleisin huolenaihe pilvipalveluista puhuttaessa on lähes poikkeuksetta epävarmuus siitä, kuinka turvassa tieto on niitä säilövän tahon hallussa. Tiedot säilötään valitun palveluntarjoajan palvelimille, joissa niiden tietoturvasta ja saatavuudesta on vastuussa ulkopuolinen taho. Yksittäisellä käyttäjällä, mutta myöskin kokonaisella yrityksellä, on hyvin vähän sananvaltaa siihen, millä mekanismeilla tiedot tulisi pitää turvassa. Mitä suurempi organisaatio on kyseessä, sitä isompi houkutus hakkereilla on päästä tietoihin käsiksi. Tämä on kuitenkin tiedostettu pilvipalveluita tarjoavien yritysten keskuudessa ja tästä syystä heidän tietoturvansa on yleensä erittäin hyvällä tasolla. Jos verrataan pientä yritystä, joka on itse vastuussa omasta tietoturvastaan ja työkseen tietoa säilövää yritystä, voidaan lähes täydellä varmuudella sanoa, että tietoturvan taso on huomattavasti heikommalla tasolla pienyrityksessä.

Palvelun toimivuus on pilvipalveluiden kohdalla yleensä yrityksen ulkopuolisen tahon vastuulla. Tämä tarkoittaa sitä, että jos verkkosivut ovat alhaalla, palvelun sisäiset komponentit eivät toimi tai tiedostoja on kadoksissa, yrityksen oman IT-osaston keinot korjata ongelma, ovat hyvin vähäiset. Yrityksen täytyy luottaa siihen, että palveluntarjoaja korjaa ongelman mahdollisimman nopeasti. Yrityksen on tärkeää selvittää, minkälainen palvelu-

taso tuotetta tarjoavalla taholla on. Palveluntasosopimus eli SLA (Service Level Agreement) on syytä neuvotella sille tasolle, että mahdollisten vikatilanteiden ilmetessä, apua saadaan mahdollisimman nopeasti. Palvelutasosopimuksen ideana on siis määritellä aikaraja sille, kuinka nopeasti ja mihin kellonaikaan yrityksen on mahdollista saada apua ongelmiinsa tuotteensa kanssa. Ennen palvelun hankkimista on tietysti myös syytä kilpailuttaa eri palveluntarjoajia ja vertailla varsinkin palveluiden ylhäällä oloaikaa.

Pilvipalvelut ovat kätevä tapa säilöä tietoa, koska tiedostojen tallennus pilveen ja niiden käyttö sen kautta onnistuu helposti. Jos pilvipalveluita käytetään ensisijaisena tallennuspaikkana, tulisi tärkeät tiedostot aina silti tallettaa myös käyttäjän omalle tietokoneelle tai muulle laitteelle. Pilvipalveluiden käyttämät komponentit, aina rautatasolta asti, ovat hyvin vahvasti liitoksissa toisiinsa, minkä takia vahingot yksittäisessä komponentissa saattavat vaarantaa koko ympäristön ja sen toimivuuden. Vaikka pilvipalvelun tarjoaja olisi itsekin vastuussa tietojen varmuuskopioinnista, ei näistä ole hyötyä siinä tilanteessa, jos koko palvelu on alhaalla. Varmuuskopiointi omalle laitteelle takaa sen, että näiden tilanteiden sattuessa, työntekijä ei ole täysin palvelun varassa, koska tiedot ovat käytettävissä myös ilman sitä.

Pilvipalvelu jakaa osittain samat riskit työpöytävirtualisoinnin kanssa, sillä pääsy käyttäjän tietoihin onnistuu täysin verkon kautta. Hakkerin päästessä käsiksi käyttäjän salasanaan, avautuu hänelle mahdollisuus kirjautua sovellukseen ongelmitta, käyttäjän tunnusta käyttäen. Luonnollisesti ennaltaehkäisy on tärkein keino taistella näitä tilanteita vastaan. Koneen asianmukainen suojaus ja viisas liikkuminen verkossa estävät haittaohjelmien pääsyn tietokoneelle. Myös kaksivaiheinen tunnistaminen on loistava tapa estää näitä tilanteita. Se edellyttää käyttäjää syöttämään käyttäjätunnuksen ja salasanan lisäksi kolmannen esimerkiksi puhelimeen lähetettävän koodin. Ilman tätä koodia, käyttäjän pääsy palveluun evätään. Tällä tavalla eliminoidaan hakkerin pääsy tietoihin, koska salasanan lisäksi, hänen tulisi anastaa myös käyttäjältä laite, kuten esimerkiksi puhelin.

5.4.4 Etätyöskentelyn riskianalyysi

Etätyön eri riskejä lähdettiin arvioimaan riskianalyysin avulla. Sen tarkoituksena on kartoittaa eri riskit, sekä arvioida niiden todennäköisyyden ja vaikutuksen kautta kokonaisriskiä. Tämän avulla pystytään määrittelemään tarvittavat toimet riskin ehkäisyyn tai paikkaukseen. Apuna tässä käytettiin taulukkoa 2.

Taulukossa 8 on esitetty etätyöskentelyn eri riskejä, niiden suuruutta sekä mahdollisia ehkäisykeinoja, joilla niiden toteutuminen voidaan välttää. Näihin riskeihin päädyttiin testauksessa esille nousseiden ongelmakohtien kautta, joita on käsitelty kappaleissa 5.4.1 - 5.4.3. Nämä ovat myös melko tavallisia, jopa arkipäiväisiä ongelmia, joista suurin osa on kuitenkin täysin hallittavissa oikeanlaisella toiminnalla. Juuri tästä syystä nämä riskit tulisi huomioida jo etätyöskentelyä suunniteltaessa. Mitä aikaisemmin ongelmat pystytään tunnistamaan ja sitä kautta ehkäisemään, sitä paremmalla tasolla tietoturva voidaan pitää. Kuten taulukosta näkee, yksikään riski ei yllä riskianalyysin korkeimmalle tasolle, mikä kuvastaa sitä, että etätyöskentely on saatu tällä hetkellä jo sille tasolle, että sen hyödyntäminen osana työskentelyä on melko tietoturvallista. Monet näistä riskeistä ovat kuitenkin vahvasti sidoksissa työntekijän omaan toimintaan. Tämän takia olisi hyvin tärkeää, että etätyöskentelyä harkitseva työntekijä saisi asianmukaisen ohjeistuksen siihen. Etätyöohjeistuksen laadinta on kertaluontoinen tehtävä, jonka jälkeen sen hyödyntäminen on hyvin helppoa.

Pilvipalveluihin siirryttäessä ja palvelimia virtualisoitaessa, yhtä suurempi osa palvelun käytettävyydestä on niitä ylläpitävän yrityksen vastuulla. Tästä syystä onkin hyvin tärkeää kilpailuttaa ja vertailla eri palveluntarjoajia ennen lopullisen sopimuksen tekoa. Hyvin usein sopimuksen teon jälkeen, yrityksellä itsellään on enää hyvin vähän sanavaltaa esimerkiksi siihen, kuinka heidän tietojansa käsitellään. Tästä syystä on oltava varma siitä, että on tyytyväinen valitsemaansa ratkaisuun.

Taulukko 8. Etätyöskentelyn riskianalyysi

Etätyöskentelyn riskianalyysi

Riski	Riskin suuruus	Ehkäisy
Käyttäjien laitteiden tietoturva	Kohtalainen	- Käyttäjien ohjeistus turvalliseen etätyöskentelyyn - Laitteiden tietoturvataso määräysten mukaiseksi - Laitteet yrityksen toimesta
Julkiset verkot	Vähäinen	- Julkisten verkkojen välttely - Verkon jako omasta puhelimesta
Käyttäjähallinnan puute	Kohtalainen	- Käyttäjätilien sulku viipymättä työsuhteen päätyttyä - Säännöllinen salasanojen vaihto
Heikko autentikointi	Merkittävä	- Kaksivaiheinen tunnistaminen - Turvatut yhteydet - Vahva virustorjunta
Palvelimien tuhoutuminen	Kohtalainen	- Palveluntarjoajien kilpailutus - Tietojen tallennus myös toiseen sijantiin
Heikko verkkoyhteys	Vähäinen	- Palveluntarjoajien kilpailutus - Tietojen tallennus myös toiseen sijantiin - Vaihtoehtoinen työskentelypaikka
Tietojen säilöminen ja niiden turvallisuus	Kohtalainen	- Arkaluontoiset tiedot vain omalla koneella - Varmuuskopiot omalle laitteelle

6 Pohdinta

Tämän opinnäytetyön tarkoituksena oli tarkastella etätyötä käsitteenä ja paneutua erityisesti kolmen eri menetelmän tietoturvaan. Nämä menetelmät valittiin sekä niiden suosion että kirjoittajan oman kokemuspohjan vuoksi. Tarkoituksena oli ottaa hyvin käytännönläheinen ote näihin menetelmiin ja toteuttaa etätyöskentelyä kaikilla eri etätyömenetelmillä muokkaamalla yrityksen sisäistä tiedostoa.

Näitä kolmea eri menetelmää tutkittiin hyödyntämällä jokaiselle räätälöityä sovellusta. Tämän avulla voitiin muodostaa selkeä kuva siitä, kuinka kukin näistä menetelmistä toimii ja mitä komponentteja se ympärilleen tarvitsee. Sovelluksia, jotka on suunniteltu tietyn etätyömenetelmän tueksi, löytyy kuitenkin useita. Vaikka niiden perustoiminta on pitkälti samankaltaista, löytyy jokaisesta silti yksilöllisiä eroja, mikä puolestaan saattaa vaikuttaa niiden tietoturvan tasoon sekä käytännöllisyyteen. Eri etätyömenetelmien tietoturvan kartoituksessa on kuitenkin pyritty ottamaan huomioon mahdollisimman kokonaisvaltaisesti kyseisen menetelmän keinot täyttää tietoturvalle asetut tavoitteet. Tästäkin huolimatta, tulokset eivät ole suoraan yleistettävissä, mikäli käytössä on jokin toinen, kuin tässä tutkimuksessa käytetty sovellus.

Eri etätyömenetelmien tietoturvaa lähdettiin arvioimaan peilaamalla niitä tietoturvalle asetettuihin tavoitteisiin sekä kartoittamalla niiden riskejä riskianalyysin avulla. Tulokset osoittavat, että etätyöskentely on työskentelymenetelmänä nykyään jo varsin tietoturvallinen. Sen suurimmat riskit ovat tällä hetkellä käyttäjälähtöisiä. Omien laitteiden käyttö ja työympäristön turvaaminen ovat hyvin pitkälti käyttäjän vastuulla. Useiden satojen työntekijöiden yrityksissä näiden osa-alueiden valvominen on haastavaa, ellei jopa mahdotonta. Itse menetelmät, joilla etätyöskentelyä toteutetaan, ovat sillä tasolla, että oikealla ylläpitokeinoilla, riskit ovat hyvin vähäiset. Koska etätyöskentelyn tietoturvariskit johtuvat pääasiassa käyttäjistä, on erityisen tärkeää tarjota heille koulutusta tai edes ohjeistusta siihen, minkälaisilla keinoilla etätyöskentely ei vaaranna heidän tai yrityksen tietoturvaa. Tähän riittää vähimmillään muutaman kohdan ohjeistus, jonka tarkoituksena on ohjeistaa käyttäjälle, kuinka tulee toimia ja mitä ei tule tehdä etänä ollessa. Mikäli etätyöskentely on arkipäivää suurelle osalla yrityksen väestä, olisi suotavaa järjestää esimerkiksi koulutuksia koko henkilökunnalle, jolloin tarvittava ohjeistus saadaan varmasti käyttäjien tietoisuuteen.

Näistä kolmesta eri etätyömenetelmästä tietoturvallisimmaksi nousi pilvipalveluiden hyödyntäminen osana etätyöskentelyä ja tässä tapauksessa erityisesti Office 365. Tämä menetelmä mahdollistaa käyttäjän pääsyn tiedostoihinsa, mistä tahansa, verkkoyhteyden avulla. Käyttäjää ei velvoiteta lataamaan ylimääräisiä sovelluksia koneellensa, vaan tie-

dostot ovat luettavissa ja muokattavissa suoraan selaimessa. Tiedostojen jako onnistuu helposti yritysten työntekijöiden kesken, oletusarvonaan kuitenkin se, että tiedostot ovat vain käyttäjän näkyvissä. Tietoturvasta vastaa tietoja säilövä yritys, jonka menetelmät niiden turvaamiseen ovat hyvin todennäköisesti paremmalla tasolla, kuin yksittäisen yrityksen. Käyttäjän tunnistaminen voidaan tehdä kaksivaiheisella autentikoinnilla, jolloin salasana lisäksi tarvitaan esimerkiksi puhelimeen lähetettävä koodi. Pilvipalveluiden kohdalla palvelusopimus takaa yleensä sen, että palvelu on lähes ympäri vuoden käyttäjän hyödynnettävissä. Esimeriksi Microsoft takaa, että heidän Office 365 palvelunsa on käytettävissä 99,9 prosenttia ajasta (Microsoft). Myös Googlen lupaa käyttäjilleen jopa 99,978 prosentin ylhäällä oloaikaa Apps for Workin kanssa (Google).

Toisaalta yritykselle, joka haluaa itse olla vastuussa mahdollisimman kattavasti kaikesta mahdollisesta, on VPN-yhteyden hyödyntäminen otollisin ratkaisu. Tällöin yritys voi itse olla vastuussa niin palvelimiensa toiminnasta, kuin VPN-yhteyteen liittyvistä konfiguraatioista. Yrityksen ei tarvitse luovuttaa tietojansa kenenkään haltuun ja datan elinkaaresta voidaan vastata omien määräysten mukaisesti. VPN-yhteyksiä tarjoavia yrityksiä löytyy markkinoilta iso määrä ja yritys voi valita näistä mieluisimman vaihtoehdon aina valmiista kokonaisuuksista avoimen lähdekoodin sovelluksiin.

Työpöytävirtualisointi pelkästään etätyöskentelyyn on liian suuri kustannuserä yritykselle kuin yritykselle. Jos vaihtoehtoa halutaan aidosti harkita, tulisi sitä hyödyntää myös toimistoympäristössä, jolloin kaikki toimiston työasemat muunnettaisiin virtuaalisiksi työasemiksi. On sanomattakin selvää, että tämä on iso muutos, jonka takia sen toimivuutta omassa yrityksessä tulee harkita tarkkaan.

Mikään ei tietysti estä yritystä hyödyntämästä useaa eri etätyömenetelmää yhdessä, jolloin päästään hyödyntämään molempien menetelmien parhaita puolia. Esimerkiksi VPN-yhteyden ja pilvipalvelun yhdistelmällä, saadaan aikaan ympäristö, jossa tietoturvallisesti arat tiedostot voidaan tallentaa yrityksen omille palvelimille ja muita tiedostoja voidaan hyödyntää pilvipalvelun kautta.

Eri etätyömenetelmiä on vertailtu niiden heikkouksien ja vahvuuksien kautta taulukossa 9. Siihen on sisällytetty niin lähteistä löytyneitä hyviä ja huonoja puolia kuin testauksen kautta esiin nousseita asioita. Kaikki taulukossa mainitut asiat ovat oleellisia oikeanlaisen etätyömenetelmän valitsemisen kannalta.

Taulukko 9. Etätyömenetelmien hyödyt ja haitat (Harbaugh 2012; Tech Blog; Viswanathan 2015)

Etätyöskentelymenetelmien hyödyt ja haitat

	VPN	Työpöytävirtualisointi	Pilvipalvelut
Hyödyt	- Käyttö helppoa konfiguroinnin jälkeen - Useita eri vaihtoehtoehtoja - Halpa - Sopii useille alustoille	- Uusien työpisteiden käyttöönotto helppoa - Hallinta helppoa - Laitteiden kustannussäästöt - Poistaa laitevarkauksien riskit	- Useiden eri laitteiden tuki - Ohjelmistojen lataus vapaaehtoista - Toinen osapuoli vastuussa palvelun ylläpidosta - Tallennustilan määrä suuri
Haitat	- Ympäristön konfigurointi vaatii paljon tietämystä - Vaatii ohjelmiston asennuksen koneille - Käyttöympäristö altistaa riskeille	- Vaatii koko työympäristön muuntamista ollakseen kustannustehokas vaihtoehto - Vaatii tehokkaita palvelimia - Työpöytien toiminta hyvin vahvasti riippuvainen palvelimista	- Käyttäjätuki suurien yritysten palveluiden kanssa heikkoa - Tietoturva jonkun toisen vastuulla

Tämän tutkimuksen jatkotutkimusmahdollisuudet painottuvat pitkälti eri menetelmien monipuolisempaan tutkimiseen. Kuten aiemmin mainittiin, tämä tutkimus toteutettiin hyödyntäen vain yhtä sovellusta tai palvelua jokaista etätyömenetelmää kohden. Varsinkin VPN-yhteyksiä tarjoavia yrityksiä löytyy useita ja näiden sovellusten toiminta saattaa poiketa oleellisesti raportissa esitetystä sovelluksesta. Raportti käsittelee myös etätyötä oikeastaan vain sen perinteisimmässä muodossa, jossa sitä hyödynnetään normaalin toimistotyön korvaajana tai vaihtoehtona. Viime vuosina etätyöskentely on kuitenkin levinnyt normaaleista toimistoympäristöistä jo kaivosalaan ja lääketieteeseen asti. Kalevi Rantanen (2016) kertoo artikkelissaan siitä, kuinka etätyötä on tullut oleelliseksi osaksi esimerkiksi kaivosalaa, jossa koneita, jotka operoivat maan alla, ohjataan useiden satojen kilometrien päästä. Tämän lisäksi jopa leikkauksia on alettu suorittamaan etänä. Jatkotutkimuksissa etätyön eri muotoja voitaisiin lähteä tutkimaan laajentamalla tarkasteltavia ympäristöjä perinteisestä toimistoympäristöstä esimerkiksi näihin yllä mainittuihin aloihin.

Opintonäytetyöprosessi eteni hyvin ja sitä saatiin edistettyä toivotulla tahdilla. Opinnäytetyötä työstettiin syksystä 2016 aina jouluun 2016 asti. Projekti aloitettiin syyskuun alussa ja se saatiin päätökseen joulukuussa. Elämänmuutokset ja työkiireet vaikuttivat projektin etenemiseen oleellisesti, sillä aikaa kirjoittamiseen löytyi yleensä vain iltaisin, muutaman tunnin ajan. Kaiken kaikkiaan suunnitellussa aikataulussa kuitenkin pysyttiin melko hyvin ja sisältöä saatiin tuotettua jatkuvalla tahdilla. Tietoturva on aihealueena hyvin laaja kokonaisuus ja sen tiettyjen komponenttien ymmärtäminen vaatii laajaa tietämystä useasta eri asiasta. Varsinkin erilaisten salausmekanismien ymmärtäminen ja niiden toiminnan hahmottaminen tuotti välillä vaikeuksia.

Opinnäytetyön tarkoituksena oli lisätä tietämystä siitä, kuinka eri etätyömenetelmät toimivat. Kiinnostus tietoturvaa kohtaan vaikutti oleellisesti aiheen valintaan ja varsinkin sen saralta tietämyksen toivottiin parantuvan. Aiemmin kokemus näistä menetelmistä oli pitkälti käyttäjälähtöistä, jolloin niiden taustalla pyöriviin mekanismeihin ei ollut sen kummemmin tutustuttu. Tieto varsinkin näistä menetelmistä ja tässä tutkimuksessa hyödynnetyistä sovelluksista kasvoi projektin aikana. Myös ymmärrys salausmenetelmistä ja niiden toiminnasta syventyi.

Kokonaisuutena opinnäytetyötä pidetään onnistuneena. Sen avulla saatiin kerättyä kattavasti tietoa eri etätyömenetelmistä sekä niiden tietoturvasta. Näiden tietojen pohjalta voitiin vetää selkeitä johtopäätöksiä, joiden perusteella etätyömenetelmän soveltuvuutta oman yrityksen työympäristöön on helppoa arvioida.

Lähteet

15Five. David Hassell. Is Remote Work Right for Your Company? Luettavissa: https://www.15five.com/blog/is-remote-work-right-for-your-company/. Luettu: 21.10.2016

Anders Innovations. 2013. Tietoturvan perusasiat pk-yrityksessä. Luettavissa: https://www.andersinnovations.com/fi/blogi/tietoturvan-perusasiat-pk-yrityksessa/. Luettu: 1.12.2016.

Beal, V. Desktop virtualization. Luettavissa: http://www.webopedia.com/TERM/D/desktop_virtualization.html. Luettu: 11.11.2016.

Boswell, W. 2016. What is an ISP? Luettavissa: https://www.lifewire.com/what-is-isp-3482410. Luettu: 30.11.2016.

Castrén, K. 2014. Turvallisen etätyön resepti. Luettavissa: https://www.tietosuoja-lehti.fi/index.php?mid=2&pid=32&aid=3396. Luettu: 6.11.2016.

Crawford, D. 2014. PPTP vs L2TP vs OpenVPN vs SSTP vs IKEv2. Luettavissa: https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/. Luettu: 16.11.2016.

Crawford, D. 2016. VPNs for Beginner – What you need to know. Luettavissa: https://www.bestvpn.com/blog/38176/vpns-for-beginners/. Luettu: 10.11.2016.

Gibilisco, S. & Haughn, M. 2014. Confidentiality, integrity, and availability (CIA triad). Luettavissa: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA. Luettu: 30.11.2016.

Google. 2016. Reliability. Luettavissa: https://support.google.com/work/answer/6056635?hl=en. Luettu: 28.11.2016.

Hanhirova, A. 2011. Mitä ovat pilvipalvelut? Luettavissa: http://gapps.fi/mita-ovat-pilvipalvelut/. Luettu: 30.11.2016.

Harbaugh, L. 2012. The Pros and Cons of Using Virtual Desktop Infrastructure. Luettavissa: http://www.pcworld.com/article/252314/the_pros_and_cons_of_using_virtual_desktop_infrastructure.html. Luettu: 1.12.2016.

Harju, E. 2010. Tietoturvasta huolehtiminen on elinehto. Luettavissa: http://www.y-lehti.fi/arkisto/artikkeli/3192/Tietoturvasta+huolehtiminen+on+elinehto+. Luettu: 1.12.2016.

Heinonen, S. 2009. Etätyön kolmas aalto liikkeelle!. Luettavissa: http://www.stat.fi/artikkelit/2009/art_2009-07-15_002.html?s=0. Luettu: 15.10.2016.

Hervasti, A. 2016. Helsingin Sanomat. Etätyön pelisäännöt vaihtelevat työpaikoilla: ”Olen ollut äärettömät yllättynyt ihmisten tunnollisuudesta”. Luettavissa: http://www.hs.fi/talous/a1473742812212. Luettu: 15.10.2016.

Hirvonen, T. 2011. Etätyön haasteiden ratkaiseminen virtualisoinnin avulla. Luettavissa: https://www.theseus.fi/bitstream/handle/10024/37293/Oppari_Tom_Hirvonen.pdf?sequence=1. Luettu: 1.12.2016.

Huikkola, S. 2016. Etätyöskentelyä helpottavia palveluita. Luettavissa: http://blog.myagent.fi/virtuaaliassistentti/etatyoskentelya-helpottavia-palveluita/. Luettu: 24.10.2016.

Janhonen, M. 2014. Etätyö haastaa johtamisen ja yhteisöllisyyden. Luettavissa: http://unelmahautomo.blogspot.fi/2014/06/etatyo-haastaa-johtamisen-ja.html. Luettu: 23.10.2016.

Järvinen, P. 2002. Tietoturva ja yksityisyys. Docendo. Jyväskylä.

Kapko, M. 2015. Google for Work vs. Microsoft Office 365: A comparison of cloud tools. Luettavissa: http://www.cio.com/article/2902255/cloud-apps/google-for-work-vs-microsoft-office-365-a-comparison-of-cloud-tools.html. Luettu: 11.11.2016.

Koivuniemi, H. 2015. Näin johdat etätyötä menestyksellisesti. Luettavissa: http://shakerlehti.fi/artikkelit/nain-johdat-etatyota-menestyksellisesti/. Luettu: 23.10.2016.

Lieke, M. 2012. Työasemavirtualisointi etätyöntekijän työasemavaihtoehtona. Luettavissa: https://www.theseus.fi/bitstream/handle/10024/45885/Lieke_Maija.pdf?sequence=1. Luettu: 1.12.2016.

Lovinus, A. 2016. What is VDI, and When Does VDI Make Sense? Luettavissa: https://blog.neweggbusiness.com/datacenter/vdi-vdi-make-sense-business/. Luettu 30.11.2016.

Lyly-Yrjänäinen, M. 2014. Työolobarometri. Luettavissa: http://tem.fi/documents/1410877/2871099/Ty%C3%B6olobarometri+syksy+2013+07022014.pdf. Luettu: 19.11.2016.

Madden, J. 2011. Desktop virtualization. Luettavissa: http://searchvirtualdesktop.techtarget.com/definition/desktop-virtualization. Luettu: 11.11.2016.

McCabe, L. 2010. What is a Virtual Desktop, and Why Should You Care? Luettavissa: http://www.smallbusinesscomputing.com/webmaster/article.php/3914891/What-is-a-Virtual-Desktop-and-Why-Should-You-Care.htm. Luettu: 11.11.2016.

Microsoft 2016. Connect to another computer using Remote Desktop Connection. Luettavissa: https://support.microsoft.com/en-us/help/17463/windows-7-connect-to-another-computer-remote-desktop-connection. Luettu: 30.11.2016.

Microsoft. Office 365 Support. Luettavissa: https://products.office.com/en-us/business/office-365-for-business-support-options. Luettu: 28.11.2016.

MTV 2013. Etätyön tekijöiden määrä saavuttanut toistaiseksi huippunsa. Luettavissa: http://www.mtv.fi/uutiset/kotimaa/artikkeli/etatyon-tekijoiden-maara-on-saavuttanut-toistaiseksi-huippunsa-/1902100. Luettu: 12.10.2016.

Nishad, M. 2015. What is the difference between web applications, web-based applications and desktop applications? Luettavissa: https://www.quora.com/What-is-the-difference-between-web-applications-web-based-applications-and-desktop-applications. Luettu: 30.11.2016.

Pekkola, J. & Uskelin, L. 2004. Etätyöopas työnantajille. Luettavissa: http://www.akava.fi/files/466/Etatyoopas_tyontajalle.pdf. Luettu: 23.10.2016.

Piispanen, V. 2006. Yriysten etäkäyttöohjelmistojen tietoturva. Luettavissa: https://www.theseus.fi/bitstream/handle/10024/11885/2006-08-22-25.pdf?sequence=1. Luettu: 1.12.2016.

Pietikäinen, S. 2013. Tietoturvallisuus – mitä se on?. Luettavissa: https://www.vahtiohje.fi/web/guest/691. Luettu: 30.10.2016.

Rahkola, A. 2013. Tietoturvallisuus etätyössä. Luettavissa: https://www.theseus.fi/bitstream/handle/10024/63445/Rahkola_Antti.pdf?sequence=1. Luettu: 1.12.2016.

Rantanen, K. 2016. Mielikuvasi etätyöstä on luultavasti vanhentunut ja se johtuu siitä, että etätyötä on kehitetty maan alla. Luettavissa: http://www.hs.fi/tiede/a1479703080552. Luettu: 28.11.2016.

Rokka, H. 2014. Miten johtaa etätyötä? Luettavissa: http://blog.kauppalehti.fi/uuden-tyon-dna/miten-johtaa-etatyota. Luettu: 23.10.2016.

Rouse, M. 2010. Wireless LAN (WLAN or Wireless Local Area Network). Luettavissa: http://searchmobilecomputing.techtarget.com/definition/wireless-LAN. Luettu: 30.11.2016.

Rouse, M. 2016. Transport Layer Security (TLS). Luettavissa: http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS. Luettu: 8.12.2016.

Rouse, M. 2016. Service-level agreement (SLA). Luettavissa: http://searchitchannel.techtarget.com/definition/service-level-agreement. Luettu: 30.11.2016.

Rouse, M. 2016. Virtual LAN (VLAN). Luettavissa: http://searchnetworking.techtarget.com/definition/virtual-LAN. Luettu: 30.11.2016.

Rouse, M. 2016. Virtualization. Luettavissa: http://searchservervirtualization.techtarget.com/definition/virtualization. Luettu: 30.11.2016.

Rouse, M. 2011. What is cloud service? Luettavissa: http://searchcloudprovider.techtarget.com/definition/cloud-services. Luettu: 11.11.2016.

Rosvall, M. 2015. Yle. Perheenäiti on tehnyt etätyötä jo kymmenen vuotta – aluksi lapset ihmettelivät. Luettavissa: http://yle.fi/uutiset/3-8361768. Luettu: 17.10.2016.
Ruohomäki, S. & Tuomivaara, V. Mitä tarkoitamme, kun puhumme etätyöstä? Luettavissa: http://www.etatyopaiva.fi/fi/artikkelit/64. Luettu: 30.11.2016.

Smith, M. 2014. How Secure Are Your Documents In Google Drive? Luettavissa: http://www.makeuseof.com/tag/how-secure-are-your-documents-in-google-drive/. Luettu: 11.11.2016.

Stanford University 2014. Liang J., Roberts J., Bloom N. & Jing Z. Does working from home work? Evidence from a chinese experiment. Luettavissa: https://people.stanford.edu/nbloom/sites/default/files/wfh.pdf. Luettu: 21.10.2016.

Subramanian, K. 2016. What is Virtualization? Luettavissa: http://karunsubramanian.com/linux/what-is-virtualization/. Luettu: 30.11.2016.

Tamminen, T. 2014. Helsingin Sanomat. Tutkimus: Avokonttorin haitat selvästi hyötyjä suuremmat. Luettavissa: http://www.hs.fi/ura/a1390024096825. Luettu: 15.10.2016.

Tech Blog. The Pros and Cons of Using a Virtual Private Network. Luettavissa: http://www.thrivenetworks.com/blog/2011/07/28/the-pros-and-cons-of-using-a-virtual-private-network/. Luettu: 1.12.2016.

Tilastokeskus 2008. Työolotutkimus 2008. Luettavissa: https://www.stat.fi/til/tyoolot/2008/index.html. Luettu: 12.10.2016.

Tilastokeskus 2015. Tietotekniikan käyttö yrityksissä 2015. Luettavissa: http://www.stat.fi/til/icte/2015/icte_2015_2015-11-26_fi.pdf. Luettu: 23.10.2016.

Torres, P. 2016. Remote Access VPN vs Site-to-Site VPN. Luettavissa: http://www.avoxi.com/blog/remote-access-vpn-vs-site-to-site-vpn/. Luettu: 11.11.2016

Työsuojeluhallinto 2013. Riskien hallinta. Multiprint Oy. Tampere. Luettavissa: http://tyosuojelujulkaisut.wshop.fi/documents/2013/11/Riskinarviointi_TSO14_2013.pdf. Luettu: 5.11.2016.

Työterveyslaitos 2014. Etätyö, eTyö, mobiili työ ja monipaikkainen työ. Luettavissa: http://www.ttl.fi/fi/muuttuva_tyoelama/tietotyon_muutokset/etatyo/sivut/default.aspx. Luettu: 12.10.2016.

Työterveyslaitos ja Suomen ympäristökeskus. Faktaa ja visiota. Luettavissa: http://www.etatyopaiva.fi/fi/faktaa. Luettu: 15.10.2016.

VAHTI 2004. Tietoturvallisuus ja tulosohjaus. Luettavissa: https://www.vahtiohje.fi/web/guest/2/2004-tietoturvallisuus-ja-tulosohjaus. Luettu: 30.10.2016.

VAHTI 2009. Etätyön tietoturvallisuusperiaatteet. Luettavissa: https://www.vahtiohje.fi/web/guest/etatyon-tietoturvallisuusperiaatteet. Luettu: 6.11.2016.

VAHTI 2009. Riskien suuruuden arviointi. Luettavissa: https://www.vahtiohje.fi/web/guest/riskien-suuruuden-arvionti. Luettu: 1.12.2016.

Viestintävirasto 2015. Laita etätyön tietoturva kuntoon. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/10/ttn201510071118.html. Luettu: 6.11.2016.

Viljanen, V. 2016. Virtuaalinen erillisverkko. Luettavissa: https://www.yksityisyydensuoja.fi/content/virtuaalinen-erillisverkko. Luettu: 10.11.2016.

Vilkman, U. 2016. Etätyön hyödyt ja haasteet johtamisen näkökulmasta. Luettavissa: http://etajohtaminen.fi/2016/02/16/etatyohon-siirtyminen-johtamisen-nakokulmasta/. Luettu: 23.10.2016.

Viswanathan, P. 2015. Cloud Computing – Is it Really All That Beneficial? Luettavissa: https://www.lifewire.com/cloud-computing-explained-2373125. Luettu: 1.12.2016.

VPN University 2016. VPN Protocol Comparison: PPTP vs OpenVPN vs L2TP vs SSTP. Luettavissa: http://www.vpnuniversity.com/learn/vpn-protocols-compared-pptp-vs-openvpn-vs-l2tp-vs-sstp. Luettu: 11.11.2016.

Vänskä, O. 2015. Näin luot vpn-yhteyden: suojaudu tiedonkeruulta ja ota hyöyty irti Netflixin kaltaisista suoratoistopalveluista. Luettavissa: http://www.tivi.fi/Uutiset/2015-01-

15/Näin-luot-vpn-yhteyden-suojaudu-tiedonkeruulta-ja-ota-hyöty-irti-Neflixin-kaltaisista-suoratoistopalveluista-3152145.html. Luettu: 10.11.2016.

Walden, S. 2015. The essential toolkit for working remotely anywhere in the world. Luettavissa: http://mashable.com/2015/07/23/tools-remote-work/#rDJdwY3F7iqi. Luettu: 24.10.2016.

Wirén, S. Etätyö edellyttää edistyksellistä viestintäpolitiikkaa, Sini Wirén, liikenne- ja viestintäministeriö. Luettavissa: http://www.etatyopaiva.fi/fi/artikkelit/10. Luettu: 30.11.2016.