LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tietoturvallisuus etätyössä

Rahkola, Antti

2013 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tietoturvallisuus etätyössä

Antti Rahkola
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2013

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Antti Rahkola

Tietoturvallisuus etätyössä

Vuosi 2013 Sivumäärä 41

Tässä opinnäytetyössä keskitytään etätyön tietoturvassa huomioon otettaviin asioihin. Yrityksessä, jossa tehdään etätyötä, on hyvä olla olemassa etätyön tietoturvaohjeistus. Työllä pyritään kehittämään työntekijöiden toimintatapoja ja parantamaan yleistä tietoturvallisuutta yrityksen sisällä.

Etätyön säännöksistä puhuttaessa viitataan vuonna 2002 käyttöön otettuun etätyön puitesopimukseen. Se on Euroopan työmarkkinajärjestöjen välinen sopimus, jossa etätyön periaatteet ja työn tekemisen ehdot on sovittu. Puitesopimusta noudatetaan sovittaessa etätyötä koskevista sopimuksista työnantajan ja etätyöntekijän välillä.

Etätyö on monille ihmisille hyvä työmuoto. Etuja ovat esimerkiksi vapaa-ajan lisääntyminen, työn ja perheen yhdistäminen, rahan ja ajan säästäminen työmatkoissa sekä saasteiden väheneminen. Myös työnantajat voivat säästää toimitila- ja laitteistokustannuksissa.

Etätyön etuja työnantajalle voivat olla imagon ja tehokkuuden paraneminen, joustavuus sekä työhyvinvoinnin lisääntyminen. Nämä asiat ovat mahdollisia saavuttaa kun työntekijällä ja työantajalla on molemminpuolinen luotto toisiinsa. Luottoa etätyön käyttönottoon lisää merkittävästi tietoturvallisuus ja juuri siksi Proactilla on tämän tyyppiselle ohjeistukselle tarvetta.

Asiasanat: tietoturvallisuus, etätyö, tietoturvaohjeistus

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

Abstract

Antti Rahkola

Information security in telecommuting

Year 2013 Pages 41

This thesis concentrates on some main issues of information security and telecommuting. It is important to have instructions about information security when telecommuting is a common practice in a company. The purpose of this guide is to improve knowledge about information security and improve the company's information security.

When talking about telecommuting, reference is commonly made to the framework agreement on telework. It is an agreement between European social organizations where the principles and conditions are agreed on. The Framework agreement is followed when contracts about telecommuting between the employer and the employee are made.

Telecommuting is a good way to work for many people. The benefits are for example: increased free time, combining family and work, saving time and money and reduced levels of pollution. Employers can also reduce costs on premises and hardware.

The benefits of telecommuting for employers are better overall image, efficiency, flexibility and employee well-being. It is possible to achieve them when there is trust between the employer and the employee. Using telecommuting as a way of working increases trust in information security and for that reason Proact Finland needs guidance of this type.

Key words: information security, telecommuting, information security guide

Sisällys

1 Johdanto

Tietoturva on perusta, jolle tärkeiden ja luottamuksellisten tietojen käsittely rakentuu. Yrityksen näkökulmasta tällaisia tietoja ovat esimerkiksi tuotteisiin, henkilöstöön, palkkoihin ja myyntiin liittyvät tiedot. Näiden yrityksen kannalta kriittisten tietojen suojaaminen ulkopuolisilta on yritystoiminnan jatkumisen edellytys. Yrityksen työntekijän kannalta tärkeitä tietoja ovat henkilökohtaiset tiedostot, työhön liittyvät dokumentit ja sähköpostiviestit, jotka nekin tarvitsevat suojaa samalla tavalla kuin yritystä koskeva tietoaineisto (Järvinen 2002, 21).

Kannettavat tietokoneet ja muut mobiililaitteet asettavat suuren haasteen nykypäivän tietoturvallisuudelle. Tietokonetta tai kannettavaa mobiililaitetta käytetään usein kaikille avoimissa julkisissa verkoissa, jolloin tietoturvallinen toiminta on oltava kunnossa. Mikäli ulkoisessa verkossa saastunut laite tuodaan takaisin yrityksen verkkoon, se voi saastuttaa yrityksen sisäisen verkon ja sitä kautta tartunnan on mahdollista levitä verkon välityksellä myös muihin yrityksen työasemiin. Tämä voi aiheuttaa yritykselle todella mittavia vahinkoja.

Yritykset ovat hyvin verkottuneita, mikä tuo uusia haasteita niin järjestelmien integroitumisen kuin tietoturvallisuudenkin kannalta. Pahimmassa tapauksessa tartunta voi levitä jopa yrityksen verkkoon yhteydessä olevaan yhteistyökumppanin verkkoon ja sen verkossa oleviin laitteisiin (Klemetti 2006).

Tässä opinnäytetyössä tutkitaan yrityksen teknisen tietoturvan osa-alueita ja sitä, mitä tulee ottaa huomioon etätyön näkökulmasta. Työ jakaantuu viiteen pääotsikkoon. Aluksi johdanto-osuudessa kerrotaan, kuinka päädyin valitsemaan juuri tämän aiheen ja miten työ on rajattu. Seuraavaksi on vuorossa kuvaus siitä mitä tällä työllä halutaan saada aikaa. Sitten esittelen tavan, jolla aihetta on lähdetty tutkimaan ja kuinka työn käytännön toteutus on edennyt. Lopuksi arvioidaan tutkimusmenetelmän soveltuvuutta tämän tyyppiseen työhön, kuinka työssä on onnistuttu ja mitkä ovat työlle luonnollisia jatkotutkimuksen aiheita.

National Sciense Foundationin omille työntekijöilleen teettämän tutkimuksen mukaan 87 % pitää etätyötä hyvänä ratkaisuna niin esimiehille, työntekijöille kuin ympäristölle. Enemmistö esimiehistä on sitä mieltä, että työntekijän tehokkuus kasvaa tai pysyy vähintäänkin samana etätyötä tehdessä (National Science Foundation 2008).

1.1 Aiheen valinta

Työskentelen järjestelmäasiantuntijana Proact Finland Oy:ssä, joka on tallennuslaitteistoihin ja tekniikoihin erikoistunut Euroopan johtava riippumaton tallennusintegraattori. Tällä hetkellä työntekijöitä on noin 50. Toimipisteitä Suomen Proactilla on Espoossa, Tampereella ja Oulussa. Proact-konsernin keskus sijaitsee Ruotsissa, josta Proact on levittäytynyt jo 12 muuhun maahan.

Lähtökohtana opinnäytetyön aihetta pohtiessani oli löytää aihe, joka on itselleni mielenkiintoinen ja josta on myös hyötyä yritykselle. Vastaavaa ohjeistusta ei ole aikaisemmin ollut käytössä, joten tämä työ tulee paikkaamaan tuon puutteen ja muistuttaa jokaista työntekijää tietoturvallisista toimintatavoista erityisesti etätyössä.

Aiheena yrityksen tietoturvan kehittäminen on mielestäni ajankohtainen ja erittäin mielenkiintoinen, ja siitä on varmasti hyötyä niin itselle kuin yritykselleKin tulevaisuudessa.

Työlle tuo lisäarvoa myös se, että iso osa työstä tehdään asiakkaan IT-ympäristössä, tietyille asiakkaille jopa etäyhteyksien välillä. Tämän vuoksi tietoturvalliset työskentelytavat ovat tärkeitä. Hyvin hoidettu ja vakuuttava tietoturva eri työskentelytilanteissa synnyttää luottamusta yrityksen ja asiakkaan välille, jolloin molemmat osapuolet voivat keskittyä työskentelemään mahdollisimman tehokkaasti (Helle 2004, 195).

Tutkimusyhtiö Coleman Parksin vuonna 2006 teettämän tutkimuksen mukaan 90 % yritysjohdosta ja 67 % työntekijöistä kokee tietoturvan haittaavan etätyötä. Suomalaisesta yritysjohdosta 55 % uskoi etätyön olevan merkittävä tietoturvauhka heidän liiketoiminnalleen. Tämän lisäksi 69 % suomalaisjohtajista koki, että työntekijät eivät huomioi tietoturva-asioita (Karvonen 2006).

1.2 Rajaus

Yleisesti tietoturvassa huomioon otettavat osa-alueet on määritelty Valtionhallinnon tietoturvallisuuden johtoryhmän(VAHTI) puolesta. Se on valtionvarainministeriön asettama johtoryhmä, joka kehittää tietoturvaa ja tekee ohjeistuksia julkisen hallinnon käyttöön. VAHTI käsittelee tietoturvaa koskevat säädökset, suositukset, ohjeet ja muut linjaukset, sekä sen tavoitteena on kehittää näiden pohjalta tietoturvallisuutta (VAHTI 2002).

Tässä työssä käsitellään etätyön tietoturvaa siihen liittyvien tietoteknisten osa-alueiden kannalta, jotka on määritelty VAHTI 2002 Valtionhallinnan etätyön tietoturvallisuusohjeessa. Tämä rajaa pois henkilöstöturvallisuuden ja fyysisen turvallisuuden. Osa-alueita, joita tämän työn ohjeistukseen sisältyy ovat: tietoliikenneturvallisuus, laitteistoturvallisuus, tietoaineistoturvallisuus, ohjelmistoturvallisuus, käyttöturvallisuus, luokitellun tiedon käsittely ja hallinnollinen turvallisuus.

1.3 Tavoitteet

Tavoitteena on tehdä etätyön ja tietoturvan yhdistävä ohjeistus, jonka mukaan yrityksen työntekijöiden tulisi toimia. Tämän lisäksi työ muistuttaa tietoturvallisista toimintatavoista, joista on hyötyä vaikka etätyötä ei tekisikään. Vain kaikille tarjolla olevan ohjeistuksen perusteella voidaan parantaa työntekijöiden tietämystä ja näin ollen myös yrityksen tietoturvaa.

Työtä voidaan käyttää myös yrityksen yleisenä tietoturvaohjeistuksena. Hyvä tilanne työn hyödyntämiseen on esimerkiksi silloin kun uutta työntekijää perehdytetään yrityksen toimintatapoihin. Työ tullaan esittelemään ja jakamaan nykyiselle henkilöstölle, jotta kaikki ovat varmasti tietoisia uudesta ohjeistuksesta.

1.4 Tutkimusmenetelmä

Kehittämistyötä aloittaessa tulee miettiä työlle soveltuva lähestymistapa, joka ohjaa työtä oikeaan suuntaan. Oikea lähestymistapa tarjoaa menetelmät, joilla päästään kehittämistyössä parhaaseen lopputulokseen. (Ojasalo 2009, 66)

Tämän työn tarkoituksena on luoda etätyön tietoturvaohjeistus yrityksen työntekijöiden käyttöön ja koulutukseen. Tämän takia päädyimme opinnäytetyön ohjaajani kanssa siihen, että tutkimustyön lähestymistavaksi soveltuu parhaiten konstruktiivinen tutkimus, jonka tarkoituksena on luoda jotain uutta olemassa olevan tiedon ja käytännössä kerättävän tiedon perusteella. Konstruktiivinen tutkimus sopii hyvin uusien tuotosten kehittämistehtäviin, kuten esimerkiksi uusi kirja, koulutusmateriaali tai www-sivusto. Tavoitteena konstruktiivisessa tutkimuksessa on saada käytännön ongelmaan ratkaisu (Ojasalo 2009, 67). Tässä tapauksessa työ tuo Proact Finland Oy:n työntekijöille uutta tietoa ja toimii mahdollisesti myös muualla kuin kohdeorganisaatiossa tietoturvaohjeistuksena.

Tutkimuksessa on kyse pyrkimyksestä muuttaa organisaation toimintaa ja käytäntöjä. Kohdeorganisaatio saa puolueettoman ja tietoon perustuvan ratkaisun ongelmaan, joka on todettu olevan olemassa. Tutkimuksen toimeksiantajan tulee jatkossa olla sitoutunut

kehittämiseen, ettei tutkimus ole vain yhden henkilön ajatus. Konstruktiivinen tutkimus ei rajaa menetelmiä tiukasti, koska tavoitteena on luoda jotain uutta niin mallista voidaan poiketa. Tutkimuksessa tarvittavaa aineistoa kannattaa kerätä monin tavoin kuten havainnoimalla, keskustelemalla ja kysymyksillä (Ojasalo 2009, 66).

Konstruktiivisen tutkimuksen prosessi voidaan jakaa kuuteen vaiheeseen. Vaiheiden noudattamisen lisäksi tulee perustella kehittämishaaste ja työn tavoitteet sekä miten työn lopputulokseen on päädytty. Konstruktiivisen tutkimuksen vaiheet ovat:

1. mielekkään ongelman etsiminen
2. syvällisen teoreettisen ja käytännöllisen tiedon hankinta tutkimuksen ja kehittämisen kohteesta
3. ratkaisujen laatiminen
4. ratkaisun toimivuuden testaus ja konstruktion oikeellisuuden osoittaminen
5. ratkaisussa käytettyjen teoriakytkentöjen näyttäminen ja ratkaisun uutuusarvon osoittaminen
6. ratkaisun soveltamisalueen laajuuden tarkastelu.

(Ojasalo 2009, 67).

1.5 Toteutus

Lähdin liikkeelle pohtimalla kuinka voisin tuoda suhteellisen lyhyen työkokemuksen avulla jotain lisäarvoa Proact Finlandin toimintaan. Työn haluttiin olevan sellainen, josta on yritykselle hyötyä ja paikkaa mahdollisia puutteita toiminnassa. Tietoturva-asiat ovat aina olleet mielenkiintoisia ja kun selvisi, että Proactilla ei oltu kiinnitetty tähän osa-alueeseen huomiota juuri ollenkaan, päädyimme tähän aiheeseen.

Syy miksi tietoturvaohjeistukseen ei ollut sen kummemmin puututtu paljastui heti tutkimuksen alkuvaiheessa. 15 vuotta IT-alalla toiminut yritys on kasvanut vähitellen IT-alan ammattilaisilla, joilla on valmiiksi olemassa vahva tietämys myös tietoturvasta. Nyt yritys on kuitenkin saavuttanut kokoluokan, jossa hallintoa ja myyntiä on noin 15 henkilöä, joilta ei enää voi olettaa hyvää tietoturvaosaamista. Tämän vuoksi ohjeistusta tarvitaan.

Tiedonhaussa lähdin liikkeelle Valtionhallinnon tietoturvallisuuden johtoryhmän(VAHTI) tekemistä aineistoista, jotka on luotu vastaamaan 2000-luvun alkupuolella lisääntyneen etätyön tarpeeseen. Näiden rinnalle halusin selkeää ja helposti omaksuttavissa olevaa informaatiota tietoturvasta, josta on hyötyä työntekijöiden jokapäiväisessä toiminnassa.

Päädyin luomaan kaksi toisistaan selkeästi eroavaa teoriaosuutta, joista teknistä tietoa on saatavilla. Turhan toiston välttämiseksi pyrin valitsemaan tietoturvan teoriaosuuteen aiheita, jotka ovat esillä päivittäisessä toiminnassa ja joihin työntekijä itse pystyy vaikuttaamaan. Näiden osa-alueiden hallinta tulisi parantamaan yrityksen tietoturvaa jokapäiväisessä toiminnassa.

Teoriaosuuden ja lähdemateriaalin pohjalta on tehty ohjeistus etätyön tietoturvan parantamiseksi. Ohjeistuksessa käydään läpi osa-alueet, jotka voidaan luokitella kuuluvaksi tekniseen tietoturvaan. Aiheen laajuuden vuoksi ohjeistus on pyritty pitäämään suhteellisen lyhyenä ja helposti ymmärrettävänä myös muille kuin IT-alan ammattilaisille.

2 Tietoturva

Tietoturvalla tarkoitetaan toimenpiteitä, joilla suojataan tietojen säilyminen ulkopuolisilta henkilöiltä koskemattomina. Tietoturvalle asetettuja tavoitteita ovat tiedon luottamuksellisuus, eheys ja käytettävyys. Näiden tavoitteiden toteutumisen mukaan voidaan tarkastella tietoturvan tasoa. (Hakala 2006, 10)

Tietoturva on hyvin laaja käsite ja se koostuu useasta eri osa-alueesta. Tietorvan osa-alueita ovat:

- Hallinnollinen turvallisuus
- Fyysinen turvallisuus
- Henkilöstöturvallisuus
- Tietoaineistoturvallisuus
- Ohjelmistoturvallisuus
- Laitteistoturvallisuus
- Tietoliikenneturvallisuus
- Käyttöturvallisuus

(Hakala 2006, 10)

”Tietoturva on investointi: Yrityksen tulee kuvatussa dynaamisessa tomintaympäristössä keskittyä bisneskriittisen datan ja toimintojen suojaamiseen. Tietoturvaa tulee ymmärtää oman liiketoiminnan kannalta. Tietoturvaan tulee suhtautua siten investointina, jolle muodostetaan strategiset suunnitelmat, joka on bisnesvetoista ja jolle laaditaan tavoitteet ja tehdään tuotos-/kustannusanalyysit, kuten mille tahansa muullekin investoinnille” (Kerttula 2000, 37).

2.1 Tietoturvan tavoitteet

Tietoturvalla pyritään suojaamaan sekä yrityksen, että työntekijöiden henkilökohtaiset ja tärkeät tiedot, joiden ei haluta joutuvan ulkopuolisten käsiin. Suojattavan kohteen päämäärät ovat seuraavat riippumatta kohteen koosta, mallista ja muodosta:

- **Luottamuksellisuus** (Confidentiality) tarkoittaa, että tiedot ovat käytettävissä vain niillä, joilla on siihen oikeus. Luottamuksellisuus saavutetaan käyttäjän tunnistuksella ja tiedon salauksella.

- **Eheys** (Integrity) tarkoittaa sitä, ettei ulkopuolinen taho pääse muuttamaan tietoa sen käsittelyn, siirron tai käytön aikana. Muutoksella tarkoitetaan esimerkiksi tiedostojen poistamista tai asiattomien muutoksien tekemistä.

- **Saatavuus** (Availability) tarkoittaa tiedon helppoa ja viiveetöntä käyttöä niille, jotka sitä tarvitsevat ja joilla on siihen oikeus. Saatavuutta voidaan uhata esimerkiksi verkkopalveluissa, jotka ovat päällä 24/7. Verkkopalvelua voidaan tarkoituksellisesti ylikuormittaa, jolloin tekoa kutsutaan palvelunestohyökkäykseksi (denial of service).

Kolmesta edellä mainitusta päämäärästä muodostuu muistisääntö C-I-A, joka muodostuu päämäärien englanninkielisistä termeistä. Päämääriä voidaan lisäksi täydentää seuraavilla osa-alueilla:

- **Kiistämättömyys** (Non-repudiaton) tarkoittaa tiedon siirtoon tai käsittelyyn osallistuneiden tunnistamista. Kiistämättömyys on erittäin tärkeää esimerkiksi sähköisessä kaupankäynnissä, jossa ostotapahtuman vaiheet pitää voida sitovasti todistaa.

- **Pääsynvalvonta** (Access Control) huolehtii siitä, että tietoon käsiksi pääsy vaatii henkilön todennuksen. Pääsynvalvonnasta vastaavat yleensä käyttöjärjestelmä ja sovellus itse.

- **Todentaminen** (Authentication) tarkoittaa varmistumista olion aitoudesta eli siitä, että olio on juuri se mikä pitääkin. Olio voi olla esimerkiksi käyttäjä, laite tai verkkopalvelu.

Tietoturvaratkaisuille ei ole olemassa yhtä oikeaa tapaa, vaan tavoitteena on löytää sopiva kompromissi, jossa vähintään edellä mainitut kolme päämäärää toteutuvat. (Järvinen 2002, 22)

2.2 Tekninen tietoturva

Laitteet ja ohjelmistot ovat merkittävä osa teknisestä tietoturvasta puhuttaessa. Tietoturva-asiat on mietittävä jo laitteistojen ja ohjelmistojen hankintavaiheessa, jotta järjestelmä saadaan turvallisesti toimintakuntoon mahdollisimman nopeasti. Tietoturvan takaamiseksi on tärkeää, että käyttöjärjestelmän sovellukset ja tietoturvaohjelmistot päivitetään säännöllisesti. Päivitykset on yleensä tarjolla ohjelmistoyritysten Internet sivuilla ja ne on helppo ladata verkon välityksellä omalle koneelle.(Kuivanen, 2005)

Työasemien ollessa yhteydessä Internetiin, on syytä varmistaa, ettei verkkoon pääse ulkopuolelta suoraan käsiksi. Tämä voidaan estää palomuurin avulla, joka hallinnoi verkkoon tulevaa liikennettä. Käyttäjien tunnistukseen käytetään usein tunnuksia ja salasanoja, mutta nekään eivät ole teknisesti aukoton ratkaisu. Tunnuksia ja salasanoja on mahdollista selvittää eri keinoin, esimerkiksi päättelyn tai tiedonsiirron aikana. Sen vuoksi on syytä noudattaa salasanojen luontiohjeita.(Kuivanen, 2005)

Teknistä tietoturvaa edistää myös tiedon salaaminen lukukelvottomaksi, jolloin tieto saadaan selville vain määritellyn purkukoodin avulla. Tiedon salaus voidaan tehdä esimerkiksi tietokoneella säilytettävälle tiedostolle, sähköpostille, verkossa välitetyille viesteille tai koko kovalevylle. Salaus voidaan tehdä monella eri menetelmällä ja eri tasolla, joka riippuu siitä kuinka vahvaksi salaus halutaan.(TAMK, 2008)

Tekniseen tietoturvaan kuuluvia tietoturvallisuuden osa-aluita ovat: tietoliikenneturvallisuus, laitteistoturvallisuus, tietoaineistoturvallisuus, ohjelmistoturvallisuus, käyttöturvallisuus, luokitellun tiedon käsittely ja hallinnollinen turvallisuus.(VAHTI, 2002)

2.3 Varmuuskopioinnin toteutus

Varmuuskopio tarkoittaa sitä että tieto on toisessa paikassa tallessa ja se voidaan sieltä tarvittaessa palauttaa.Varmuuskopiointi on tärkeä osa yrityksen teknistä tietoturvaa. On tärkeää, että vahingon sattuessa tiedot pystytään palauttamaan aiemmin valliinneeseen tilanteeseen tietoja menettämättä. (Oulun Yliopisto, 2012)

Tiedostojen tuhoaminen on yksi yleisimmistä haittaohjelmien toiminnoista, koska se on erittäin vahingollista ja suhteellisen helppo toteuttaa. Vaarana on myös tiedostojen poistaminen vahingossa ja viruksen aiheuttama tiedostojen katoaminen. Lisäksi tallennuksessa käytettävään kovalevyyn tai ulkoiseen muistiin voi tulla fyysinen tai tekninen vika, jolloin ne eivät enää toimi ja tiedostoja on mahdotonta käyttää. Kannettavien laitteiden kohdalla riskiksi muodostuvat myös varkaudet, joiden vahinkoja varmuuskopioilla voidaan vähentää huomattavasti.(Oulun Yliopisto, 2012)

Tietojen varmuuskopiointiin voidaan käyttää tarpeesta ja laitteesta riippuen eri tapoja. Esimerkiksi Cd tai dvd-levyjä, joilla suurienkin tiedostojen varmuuskopioiden tallentaminen on nopeaa. Usein toistuva kopiointi käy kätevästi myös USB-liitäntään kytkettävän ulkoisen kiintolevyn avulla. Kovalevyn rikkoutumisen tai haittaohjelmien tekemän tuhoamisen jälkeen järjestelmä on helppo palauttaa, jos siitä on täydellinen varmuuskopio.(Oulun Yliopisto, 2012)

Yleensä ei kuitenkaan kannata kopioida koko kovalevyä, koska käyttöjärjestelmä ja useimmat sovellusohjelmat voidaan asentaa uudestaan alkuperäisiltä levyiltä tai ladata tietokoneelle uudestaan Internetistä. Koko kovalevyn varmistaminen vaatii myös tilaa ja resursseja paljon enemmän, joten olisi syytä varmuuskopioida vain siihen luokitellut tiedot.(Webopas, 2012)

Erittäin tärkeistä tiedostoista kannattaa ottaa useampia kopioita ja säilyttää niitä fyysisesti eri paikoissa. Mikäli joku versio tiedostosta tuhoutuu esimerkiksi tulipalossa, säilyy toinen kuitenkin vahingoittumattomana. Kopioiden säilytyspaikan on hyvä olla myös sellainen, etteivät ne pääse vahingossa tuhoutumaan esimerkiksi auringonvalossa, voimakkaassa magneettikentässä tai jää esimerkiksi kaatuvan kahvikupin alle.(Kuivanen, 2005)

Varmuuskopioita on muistettava ottaa säännöllisesti ja riittävän usein, jotta tallessa on aina tuore versio tiedostoista. Varmistukset voi myös automatisoida käyttöjärjestelmän työkaluilla tai tallennukseen suunnitelluilla ohjelmilla. Tiedostoja ei kannata tallentaa vanhan päälle vaan ne tulee versioida ja nimetä järkevästi, jolloin kopioiden ylläpito ja säilytys helpottuu, koska tiedostot ovat hyvin järjesteltynä.(Oulun Yliopisto, 2012)

2.4 Tiedon salaus

Tietojen salauksella voidaan varmistaa tietojen luottamuksellisuuden säilyminen. Tiedostojen salausta hyväksikäyttävien sovellusten avulla on mahdollista varmistaa myös tietojen eheys sekä eri järjestelmien tai käyttäjien välisten vuorovaikutusten kiistämättömyys. Tämä tarkoittaa esimerkiksi sitä, että voidaan varmistua tietyn sähköpostiviestin lähettäjästä. (Laaksonen, 2006)

Salaustekniikoiden käyttäminen vaatii järjestelmiltä laskentatehoa mikä tekee järjestelmistä ja niiden hallinnasta hieman monimutkaisempia. Salauksesta on myös se haitta, että verkossa olevat tietoturvasovellukset, kuten palomuurit, eivät useinmiten voi tutkia salattua verkkoliikennettä. Tämä on mahdollista vain siten että palomuuri itse osaa purkaa ja uudelleen salata tiedot kyseisessä laitteessa.(Laaksonen, 2006)

Tiedostojen salaukseen löytyy lukuisia ohjelmia ilmaisista maksullisiin, jotka vaihtelevat jonkin verran ominaisuuksiltaan. Tiedostojen salaukseen käytettäviä ohjelmistoja voi ladata internetistä ohjelmistojen kotisivuilta tai ne voi hankkia tietotekniikan alan liikkeistä. Microsoftilla on uusimmissa käyttöjärjestelmissään oma tiedostonsalausohjelma, jonka käyttöön löytyvät tarvittaessa ohjeet Microsoftin tukisivustoilta.(Laaksonen, 2006)

Tiedostoja voidaan salata myös salaamalla tietokoneen koko kovalevy. Tällöin voidaan estää ulkopuolisten henkilöiden pääsy koneelle tallennettuihin tietoihin esimerkiksi varkaustapausten yhteydessä. Kiintolevyn salaus ei haittaa tietokoneen käyttöä millään tavalla. Salausohjelmistoa valittaessa tulee varmistaa, että valittu ohjelmisto mahdollistaa keskitetyn ylläpidon ja erityisesti palautusavaimen käytön, jonka avulla voidaan tarvittaessa asettaa käyttäjälle uusi salasana.(Laaksonen, 2006)

2.5 Palomuuri

Palomuuri on laitteistolla, ohjelmistolla tai niiden yhdistelmällä toteutettava suoja, jolla valvotaan verkkojen ja verkossa olevien laitteiden välistä liikennettä. Palomuurilla pyritään estämään verkon välityksellä tapahtuva luvaton liikennöinti työasemiin ja tietojärjestelmiin. Kotikätössä palomuurit suojaavat tietokonetta kotiverkon ja Internetin välillä. Tällaiset kotipalomuurit ovat yleensä tietokonesovelluksia, jotka ovat nykyään sisäänrakennetteuina useimmissa käyttöjärjestelmissä.(Kuivanen, 2005)

Suuremmissa organisaatioissa palomuurit suojaavat sisäverkkoa ulkoverkosta tulevilta hyökkäyksiltä. Tällaiset palomuurit on usein toteutettu laitteistolla, koska palomuurin on oltava jatkuvasti päällä suojaamassa yrityksen verkkoa ja siellä kiinni olevia laitteita. Laitteistopalomuurin eduksi voidaan laskea myös sen hallinnan helppous mikäli yrityksen verkossa on useita tuhansia työasemia.(Kuivanen, 2005)

Laitteistopalomuurin lisäksi työvälineet tulee suojata työaseman omalla palomuurisovelluksella. Palomuuria voidaan käyttää myös verkossa liikennöinnin seuraamiseen, sillä kaikki verkkoliikenne kulkee palomuurin läpi. Yrityksen tietoverkoissa on tärkeää hallita mistä yhteyksiä sallitaan ja mitkä portit liikenteelle ovat auki.(Kuivanen,2005)

Palomuuri ei kuitenkaan suojaa kaikelta verkosta tulevalta haitalta, sillä se ei puutu verkkoon tulevan liikenteen sisältöön. Mikäli verkkoon pääsee palomuurin läpi, ei palomuurista ole enää estämään viruksen tai muun tunkeutujan tuhoja. Tähän tarvitaan virustorjuntaa. (Kuivanen, 2005)

2.6 Virustorjunta

Virustorjunta on tärkeä osa suojautumisessa verkossa leviäviä haittaohjelmia vastaan. Yritysverkossa virustorjunta asennetaan kohtiin, joista Internetin kautta tuleva liikenne kulkee, kuten palomuuriin.(Panda Software Finland, 2012) Yritysten virustorjunta toteutetaan yleensä automaattisilla järjestelmillä, joita hallitaan keskitetysti esimerkiksi tietohallinnon toimesta. Päivitykset voidaan asentaa ilman käyttäjän vaivaamista ja ohjelmisto on aina ajan tasalla. (Humak, 2009)

Virustorjunta toimii käytännössä kahdella tavalla. Yleisin tapa on skannata koko kone läpi tutkien kaikki tiedostot virusten varalta. Skannaus voi olla ajastettu tai sen voi ajaa itse silloin kun haluaa. Skannaukseen voi määritellä tietyt tiedostomuodot, levyasemat ja kiintolevyt, joilta haku tehdään. Virusten hakuun ohjelma käyttää tunnistetietokantaa. (Gercek, 2008)

Ohjelmistosta riippuen on mahdollista käyttää myös taustavalvontaa, joka on jatkuvasti päällä työaseman taustalla. Toiminto valvoo kaikkia koneeseen saapuvia ja koneesta lähteviä tiedostoja sekä tutkii tiedostot, jotka tallennetaan kiintolevylle. Taustavalvonta hyödyntää myös samaa tunnistetietokantaa kuin skannaus. Sen vuoksi virustorjuntaohjelmisto on erittäin tärkeää pitää ajan tasalla asentamalla kaikki päivitykset heti niiden julkaisun jälkeen. (Gercek, 2008)

Näiden perustoimintojen lisäksi jotkut ohjelmistot käyttävät heuristista tutkimusjärjestelmää, joka käyttää keinoälyteknologiaa virusten tunnistamiseen. Järjestelmä pyrkii tunnistamaan automaattisesti ohjelmistossa havaitut epänormaaleiksi luokiteltavat ilmiöt. (Gercek, 2008)

2.7 Käyttäjätunnukset ja salasanat

Käyttäjätunnukset ja salasanat koostuvat joukosta kirjaimia ja numeroita, joilla tietojärjestelmä todentaa käyttäjän tunnistuksen. Käyttäjätunnus toimii tietojärjestelmissä käyttäjän yksilöivänä tunnisteena. Tunnus voidaan muokata esimerkiksi käyttäjän etu- ja sukunimesta tai se voi olla jokaiselle käyttäjälle määritelty vakio, kuten esimerkiksi henkilökohtainen sähköpostiosoite. Käyttäjätunnukset ovat monissa tietojärjestelmissä julkisia, jolloin tunnukseksi voidaan keksiä henkilöllisyyden salaamiseksi mikä tahansa kirjainyhdistelmä.(Kuivanen, 2005)

Tunnuksen perusteella voidaan määritellä myös käyttöoikeuksia. Peruskäyttäjä ei yleensä tarvitse oikeuksia kuin tiettyjen sovellusten käyttöön ja omaan kotihakemistoon, joka Windows ympäristössä löytyy Omat tiedostot alta ja Linuxissa /home hakemistosta. Käyttäjätunnukselle annettavien oikeuksien kanssa kannattaa olla tarkkana sillä haittaohjelman päästessä koneeseen se käyttää samoja oikeuksia, joilla koneelle on kirjauduttu. Tämän vuoksi esimerkiksi pääkäyttäjänä(administrator) ei tulisi työskennellä lainkaan edes kotikoneella.(Kuivanen, 2005)

Salasanalla tunnistaudutaan yleensä kaikkiin tietojärjestelmiin. Sen vuoksi on erittäin tärkeää että ulkopuoliset eivät pysty sitä arvaamaan ja pääse käsiksi esimerkiksi sähköpostiin tai käyttäjän henkilökohtaisiin tiedostoihin. Vaikka omissa tiedoissa ei olisikaan mitään salattavaa, heikentää helposti arvattava salasana koko järjestelmän tietoturvaa. Jokaiseen tietojärjestelmään tulisi aina käyttää eri salasanaa.(Kuivanen, 2005)

2.7.1 Hyvä salasana

Hyvä salasana on tehokas tietoturvan parantaja. Salasanan tulee olla juuri niin vaikea, että sen muistaa itse mutta ei ole muiden arvattavissa. Sen ei siis tarvitse olla joukko täysin satunnaisia kirjaimia ja numeroita, jolloin houkutus kirjoittaa se muistiin kasvaa suureksi. (Helsingin Yliopisto, 2012)

Salasana ei tulisi olla johdettavissa nimestä tai käyttäjätunnuksesta, sillä näitä hyökkääjät kokeilevat ensimmäiseksi. Salasanan ei tule myöskään olla mitään omaan elämään liittyvää, kuten auton rekisterinumero, syntymäaika, puhelinnumero tai lapsen nimi. (Järvinen 2002, 340)

Englantilaisen Egg-pankin vuonna 2002 tekemän tutkimuksen mukaan suuri osa asiakkaitten salasanoista on helposti arvattavissa, sillä ne liittyvät jollain tavalla omaan elämään tai mielenkiinnon kohteisiin. Usein salasanat ovat myös helposti arvattavia yhdistelmiä näistä tutuista asioista.

Asiakkaiden salasanat

- 23 % lapsen nimi
- 19 % kumppanin nimi
- 12 % syntymäpäivä
- 9 % jalkapallojoukkue
- 9 % julkkis tai bändi
- 9 % paikannimi
- 8 % oma nimi
- 8 % lemmikin nimi

Egg-pankin selvitys 1000 asiakkaan salasanoista (Järvinen 2002, 340).

Floridan yliopistossa tehdyn tutkimuksen mukaan turvattomat salasanat ovat yhä suosittuja, vaikka niistä luonnin yhteydessä mainitaan lähes joka paikassa.Tutkimuksen aineistona käytettiin 32 miljoonaa hakkerin varastamaa salasanaa, joiden perusteella selvisi, että joka viides internetin käyttäjä tyytyy yksinkertaiseen salasanaan. Salasanoissa toistuvat vuodesta toiseen samat sanat. Tutkijoiden mukaan 5000 suosituinta sanaa esiintyy 20 prosentissa salasanoista. Tällaiset salasanat ovat melko helposti murrettavissa, sillä hakkerit pystyvät käyttämään suosituimpia sanoja ja niiden muunnoksia sekä tekemään tuhansia salasana-arvauksia minuutissa siihen tarkoitukseen tehtyjen sovellusten avulla (Repo, 2010).

Salasanojen tietoturvavaaroista on puhuttu jo pitkään mutta oppi ei näytä menevän perille. Tutkijoiden mukaan se johtuu siitä, että nykyään on niin paljon muistettavaa. Sen vuoksi salasanat halutaan pitää helppoina ja samoja sanoja käytetään monissa paikoissa. Tärkeää tietoa sisältävien palveluiden, kuten pankkisivujen salasana tulisi kuitenkin olla huolella mietitty. Sen sijaan esimerkiksi viihdesivuilla ja sivuilla missä ei jaeta mitään henkilökohtaista tietoa voidaan käyttää yksinkertaisempaa salasanaa (Repo, 2010).

2.7.2 Salasanan luominen

Salasanan on hyvä olla vähintään kahdeksan merkkiä pitkä ja sen tulisi sisältää sekä isoja että pieniä kirjaimia ja numeroita. Se ei saisi olla mikään kielessä esiintyvä sana tai nimi. Sen ei tulisi myöskään liittyä omaan työhön, harrastuksiin, perheeseen, toimintaan, olemukseen tai muihin itseensä viittaavaan asiaan (Helsingin Yliopisto, 2010).

Hyvien salasanojen luontitapoja on useita. Tässä muutamia esimerkkejä:

- kaksi toisiinsa liittymätöntä sanaa erotettuna esimerkiksi numeroilla
- pienten ja isojen kirjainten sekoitus
- merkkijono, joka näyttää päällepäin satunnaiselta mutta onkin joku keksitty oma sana takaperin ja isoilla kirjaimilla sotkettuna
- merkkijono, joka näyttää satunnaiselta mutta onkin joku sana kirjotusvirheellä ja numerolla sotkettuna
- merkkijono, jonka kirjaimista muodostuu itse keksitty lause esimerkiksi englanniksi.

(Helsingin Yliopisto, 2010)

2.7.3 Salasanojen tallennus

Kaikista paras salasanojen tallennuspaikka on salasanojen painaminen omaan mieleen, eikä missään tapauksessa kirjoittaminen muistiin. Salasanoja ei pidä kirjoittaa paperille, eikä myöskään tietokoneelle tekstitiedostoon.
Salasanoja voi kuitenkin olla monia, jolloin kaikkien muistaminen ulkoa ei ole välttämättä mahdollista. Tällöin voidaan käyttää salasanojen tallennusohjelmia, jolloin salasanoihin päästään käsiksi muistamalla vain yksi täydellinen salasana. Verkossa on myös tarjolla salasanojen tallennuspalveluita, jolloin salasanoihin on turvattu pääsy ympäri vuorokauden ja mistä tahansa.(Symantec, 2008)

2.7.4 Salasanan vaihtaminen

Hyvissä tietojärjestelmissä salasanan vaihtaminen on pakollista tietyin aikavälein. Järjestelmä ilmoittaa salasanan vanhenemisesta, jolloin salasana on syytä vaihtaa heti.
Tietojärjestelmästä tai kohteesta riippuen salasana kannattaa vaihtaa 1-6 kuukauden välein. Salasana kannattaa aina kehitellä kokonaan uusiksi, sillä muuten vaihtamisen tuoma tietoturvallisuus heikentyy huomattavasti.(Symantec, 2008)

2.8 Haittaohjelmat

Teknisten ongelmien ja hakkereiden lisäksi myös virukset ja haittaohjelmat aihettavat käyttäjille vaivaa levitessään tietoverkoissa koneesta toiseen. Virukset eroavat hakkereista siinä, että ne leviävät aina käyttäjien toiminnan seurauksena. Kaikista paras suojautumiskeino virustorjuntaohjelmien ollessa kunnossa on käyttäjän oma varovaisuus ja tarkkaavaisuus.(Järvinen 2002, 249)

Sivustoilla surffailtaessa ei välttämättä kannata avata jokaista linkkiä ja esiin ponnahtavaa ikkunaa. Pelkästään tällaisella toiminnalla voidaan välttyä isoilta ongelmilta, sillä haittaohjelmat tarvitsevat vain yhden klikkauksen käyttäjältä aktivoituakseen.

2.8.1 Virukset ja madot

Virukset ja madot ovat vahingollisia tietokoneohjelmia, jotka on ohjelmoitu leviämään tietoverkoissa. Molemmat etenevät levittämällä itsestään kopioita, mikä tapahtuu usein koneen käyttäjän avustuksella. Virus toimii yleensä kahdessa vaiheessa. Ensin se levittää itsestään kopioita koneesta koneeseen tietoverkkojen välityksellä. Toisessa vaiheessa se aktivoituu ja alkaa tekemään tuhojaan, joita siihen on ohjelmoitu.(Suomen Internetopas, 2010)

Madot ja virukset eroavat toisistaan siinä, että virus kätkeytyy ohjelman sisään, jolloin se tarvitsee jonkinlaisen aktivoinnin käynnistyäkseen. Aktivointi voi tulla huomaamatta esimerkiksi koneen käyttäjältä. Mato taas leviää omin voimin käyttämällä avukseen Internetiä ja käyttöjärjestelmien tietoturva-aukkoja, eikä se välttämättä yritäkään piiloutua. (Kuivanen, 2004)

Virukset ja madot voivat tarttua muihin ohjelmatiedostoihin tai koneen käynnistysohjelmaan, joka sijaitsee kovalevyllä. Käynnistyslohkoon päästessään tuhot voivat olla todella suuret, eikä käyttöjärjestelmään pääse välttämättä ollenkaan. Sähköpostivirukset leviävät sähköpostin liitetiedostojen välityksellä ja osaavat lähettää itsensä eteenpäin koneelta löytyviin osoitteisiin. Virus voidaan ohjelmoida tuottamaan haittaa, jolloin se tuhoaa tiedostoja tai tietoja tarkoituksellisesti. Usein viruksen tai madon pelkkä leviäminen tuottaa käyttäjälle haittaa tietokoneen jumiutumisen ja internet-liikenteen hidastumisen muodoissa. (Suomen Internetopas, 2010)

2.8.2 Troijalaiset ja takaovet

Troijalainen on yleensä pienehkö ohjelma, joka on naamioitu aivan normaaliksi hyödylliseksi sovellukseksi. Tällä ohjelmalla voi jopa suorittaa jotain toimintoja mutta samalla se aktivoi viruksen, madon tai muun haavoittuvuuden tietojärjestelmään. Keino troijalaisten poistamiseen on virustorjuntaohjelma, joka tutkii koko koneen tiedostot läpi ja antaa ilmoituksen troijalaisen löytyessä sekä laittaa sen vähintään karanteeniin.(Datta, 2012)

Troijalaiset pystyvät myös lähettämään tietoa koneella tapahtuvasta toiminnasta kolmansille osapuolille. Se voi tallentaa esimerkiksi kirjoitetut salasanat, tunnukset ja luottokortin numerot tallentamalla kaiken mitä näppäimistöllä kirjoitetaan. Nuo tiedot troijalainen lähettää eteenpäin sitä hallitseville henkilöille.(Datta, 2012)

Tänä päivänä isoon osaan troijalaisista on ohjelmoitu niin sanottu botnet toiminnallisuus. Botnet on iso joukko saastuneita koneita, joita troijalaisen hallitsija käyttää esimerkiksi massalähetyksiin ja palvelunestohyökkäyksiin(DDoS). Tällaiset lähetykset kuormittavat verkkoa todella paljon ja tarpeeksi suurina määrinä kaatavat kokonaisia verkossa toimivia palveluja.(Datta, 2012)

Takaovi tietokoneessa tarkoittaa normaalin oikeutetun käyttäjän todennuksen ohitusta, jota kautta krakkeri pääsee koneeseen käsiksi. Koneen hallinta tapahtuu esimerkiksi jonkun saastuneen sovelluksen varaaman portin kautta, jonka krakkeri löytää. Krakkeri ottaa yhteyden sovelluksen hallitsemaan porttiin ja pystyy sen jälkeen hallitsemaan konetta sekä näkee kaiken tapahtuvan verkkoliikenteen. Takaovi voi olla sovellus itsessään, muokattu osa sovellukseen tai laite koneessa. Takaovet ovat lähteeneet liikkeelle suoraan sovelluskehittäjistä, jotka ovat jättäneet kirjoittamaansa sovellukseen takaoven joko tarkoituksella tai vahingossa.(University of Amsterdam, 2012)

2.8.3 Mainos- ja vakoiluohjelmat

Mainosohjelmat ovat haittaohjelmien kategoriassa sieltä haitattomasta päästä kun pysyttelee avaamatta näytölle aukeavia mainosikkunoita, joka saattaa johtaa jonkin haitallisemman ohjelman latautumiseen tai aktivoitumiseen. Mainosohjelmat keräävät tietoa käyttäjän kiinnostuksen kohteista esimerkiksi internetin selaustietojen perusteella. Näin muodostuu profiili, jonka mukaan mainosohjelma alkaa näyttämään juuri tälle profiilille suunnattuja mainoksia (RM Education, 2009)

Nimensä mukaisesti vakoiluohjelma on sovellus joka vakoilee koneella tehtäviä asioita huomaamattomasti taustalla, jolloin käyttäjä ei sitä huomaa. Se pyörii todennäköisesti käyttöjärjestelmässä taustalla, eikä se aiheuta peruskäyttäjälle mitään näkyvää toimintaa. Vakoiluohjelma voi olla esimerkiksi sellainen, että se tallentaa käyttäjän jokaisen napinpainalluksen ja lähettää ne eteenpäin. Tämän jälkeen painalluksista päätellen voidaan saada salasana tai käyttäjätunnus selville. Vakoiluohjelma voi myös seurata käyttäjän selaamia internet- ja sähköposti-osotteita ja lähettää sähköposteja käyttäjän sähköpostitilin osoitteisiin. Yleisimmin tällainen ohjelma tulee koneelle jonkin muun ohjelman yhteydessä, käyttäjän huomaamatta tai klikkaamalla nettisivulla haitallista linkkiä, jolloin ohjelma latautuu automaattisesti koneelle.(Datta, 2012)

2.9 Sähköpostin tietoturva

Sähköposti on viestien lähetysjärjestelmä, jolla voidaan siirtää tekstiä ja liitetiedostoja tietoverkkojen välityksellä ympäri Internetiä. Posti kulkee verkossa erittäin nopeasti ja on luettavissa missä vaan esimerkiksi mobiililaitteen tai tietokoneen avulla. Sähköpostin lähettäminen on ilmaista, mikä on johtanut sähköpostin turhaan lähettämiseen ja verkon kuormittumiseen. Pahiten tämä nousee esille mainostajien lähettämissä mainospostissa ja roskapostissa, jota syyttömien vastaanottajien postilaatikot keräävät pahimmissa tapauksissa satoja päivässä.(Järvinen 2002, 215)

Sähköpostin käytön perusteita:

- Lähettäjän nimikentän tietoon ei voi täysin luottaa. Lähettäjän aitous tulee varmistaa jos on pientäkin syytä epäillä sitä.
- Viestin perillemenosta voi olla varma vasta silloin, kun vastaanotta on kuitannut saaneensa sen.
- Tärkeat viestit tulee lähettää salattuina.
- Kerran lähetetty sähköpostiviesti voi jäädä talteen useiksi vuosiksi ja toimii kirjallisena todisteena. Harkitse, mitä lähetät.
- Älä käytä työpaikan sähköpostia yksityisiin viesteihin, vaan ohjaa ne johonkin webmail-palveluun. Näin postit pysyvät järjestyksessä, eivätkä yksityiset asiat ja työ sekoitu keskenään.

Sähköpostiviestit kulkevat verkossa eri tekniikoiden avulla. Verkkoon lähetetty sähköposti löytää perille nimipalvelimen avulla, joka kertoo missä suunnassa on vastaanottajalle menevää postia käsittelevä sähköpostipalvelin. Sähköpostipalvelin jatkaa postin yrityksen verkkoon ja sieltä edelleen asianomaiselle henkilölle(Järvinen 202, 216).

Sähköposti välitykseen käytetään usein SMTP-protokollaa ja postin lukemiseen sähköpostisovellukset käyttävät yleensä POP3 ja IMAP protokollia. Myös HTTP-protokollaa käytetään lukemisessa kun lukeminen tapahtuu selaimen avulla (Klensin, 2001).

2.9.1 Sähköpostin salaus

Sähköpostin salaaminen on sen sisällöstä riippuen erittäin tärkeää, koska sähköpostiviestit ovat kaikkien niiden luettavissa, jotka pystyvät kuuntelemaan verkon sisäistä liikennettä. Sähköpostin luottamuksellisuus ja eheys voidaan säilyttää salaamalla viesti, sekä allekirjoittamalla se digitaalisesti. Tällöin voidaan varmistua viestin lähettäjän henkilöllisyydestä. Sähköpostin perustason suojauksen voi tarkistaa selaimen osoitteesta. Kun se on Https alkuinen ja selaimessa on näkyvissä lukon kuva on yhteys SSL-suojattu. (Viestintävirasto, 2013

Sähköpostien salaamiseen ja allekirjoittamiseen on tarjolla useita erilaisia ohjelmia. Ohjelmista tunnetuin on PGP (Pretty Good Privacy). Ohjelman avulla käyttäjä voi lähettää ja vastaanottaa luottamuksellisiä sähköpostiviestejä ja niiden liitteitä, sekä viestit voidaan varmentaa ja allekirjoittaa. PGP toimii siten, että se salaa viestin vastaanottajalta saamallaan julkisella avaimella, jonka jälkeen vastaanottaja saa viestin auki omalla yksityisellä avaimellaan, joka vastaa tuota julkista avainta. Vaikka kolmas osapuoli onnistuisikin kaappaamaan sähköpostin, ei hän pysty lukemaan itse viestiä. PGP luo avaimet asennuksen yhteydessä. (Järvinen, 2005)

Sähköpostiviestin allekirjoitus toimii samalla periaattella. Siinä lähettäjä allekirjoittaa viestin omalla yksityisellä avaimellaan, jolloin vastaanottaja voi todentaa viestin lähettäjän julkisen avaimen avulla. (Viestintävirasto, 2013)

Myös pelkkä liitetiedosto voidaan salata käyttämällä sovellusten omia salasanatoimintoja, jolloin viestiksi kirjoitetaan saate ja lähettäjä ilmoittaa aavaamiseen tarvittavan salasanan esimerkiksi henkilökohtaisesti ja puhelimitse. (Järvinen, 2005)

2.9.2 Sähköpostin liitetiedostot ja roskaposti

Pelkällä sähköpostin huolellisella käytöllä voidaan välttää uhkaavia tietoturvariskejä ja virusten leviämistä tietoverkossa. Sähköpostiviestien sisältämiä tuntemattomia liitteitä ei tulisi koskaan avata, ellei lähettäjästä ole täyttä varmuutta. Käyttäjät houkutellaan avaamaan liitetiedosto, jolloin se aktivoi viruksen tai haittaohjelman. (Tietoturvaopas, 2012)

Kaupusteluviestit ovat nykyään suuri osa sähköpostiliikennettä ja ennen pitkää lähes jokaiseen postilaatikkon rupeaa tulemaan mainoksia, joita ei ole tilannut. Viesteihin ei pidä koskaan vastata sillä se lisää itselle tulevan roskapostin määrää. Tämä johtuu siitä, että vastaamisen jälkeen yhä useampi tili tietää osoitteesi olemassaolosta. Roskaposteja lähetetään usein kiertokirjeiden muodossa, joten kiertokirjeiden lähettäminenkään ei ole suositeltavaa. (Tietoturvaopas, 2012)

Roskapostilla mainostettavat tuotteet ovat usein hyvin epämääräisiä tai jopa laittoimia. Posteissa voidaan luvata esimerkiksi nopeaa rikastumista, keinoa päästä eroon veloista tai ihmelääkkeitä eri sairauksiin. Markkinoinnin tekeminen roskapostin avulla ei maksa lähettäjälle mitään, minkä vuoksi sitä lähetetään rajattomia määriä. (Järvinen 2002, 235)

Roskapostilta suojautuminen on melko vaikeaa mutta seuraavassa joitain keinoja siihen.

- Poista viestit heti niiden saavuttua ja niitä turjaan avaamatta.
- Poista nimesi jakelulistalta mikäli siihen on mahdollisuus.
- Lisää lähettäjä sulkulistalle, jolloin samasta paikasta lähetetyt viestit eivät pääse perille.
- Käytä torjuntaohjelmia, jotka estävät ja poistavat roskapostiviestit automaattisesti.
- Tee ilmoitus lähettäjän operaattorille.
  (Järvinen 2002, 237)

Liitetiedostot voivat sisältää monenlaisia haittaohjelmia ja saastunut liitetiedosto onkin yksi yleisimmistä haittaohjelmien leviämistavoista. Ensimmäisenä luottamattomalta lähettäjältä tulleesta viestistä tulee tarkistaa, että liitetiedosto ei ole ohjelmatiedosto, joka avattaessa suorittaisi itsensä suoraan. Tällaiset tunnistaa tiedostopäätteistä: .exe, . com, .bat, .cmd, .scr, .pif. Tiedosto voi olla myös pakattuna .zip tai .rar muotoon käyttäjän hämäämiseksi. (Tietoturvaopas, 2008)

2.9.3 Phishing

Phishing:llä (Password Fishing) tarkoitetaan erilaiset tunnusten ja salasanojen laitonta hankkimista käyttäjää huijaten. Yleensä huijaus kohdistuu johonkin taloudellisesti merkittävään tietoon kuten: verkkopankkitunnukseen, luottokorttinumeroon tai henkilötietoihin. Tietojen kalastelua tehdään pääasiassa sähköpostin välityksellä. Viesti yritetään naamioida siten, että käyttäjä luulee sen tulleen viralliselta taholta kuten pankin asiakaspalvelusta. Www-sivustot, jonne taloudellista tietoa pyydetään luovuttamaan, voivat olla ulkoisesti esimerkiksi täysin verkkopankin sivujen näköiset. Todellisuudessa nämä sivustot ovat kuitenkin phishing-hyökkääjän haltuunottamaan tietojärjestelmään luomia huijaussivustoja, jonne syötetyt tiedot päätyvät tietojen kalastelijan käsiin. (Cert-Fi, 2007)

Sähköpostiviesteissä tulee ottaa huomioon, että pankit eivät koskaan kysy tunnuslukuja tai muita henkilökohtaisia tietoja sähköpostin avulla. Myöskään lähettäjätietokentän sisältöön ei voi luottaa täysin, koska se voidaan helposti naamioida näyttämään pankin osoitteelta. (Cert-Fi, 2007)

Phishing-viesteiltä suojautuminen:

- Älä avaa epäilyttävältä näyttäviä sähköpostiviestejä.
- Älä siirry minkään sähköisen asiointipalvelun sivuille sähköpostissa tai pop-up ikkunassa olevan linkin kautta. Turvallisin tapa siirtyä esimerkiksi verkkopankin sivuille on kirjoittaa osoite itse osoitetietokenttään.
- Tarkista ennen palveluun kirjautumista, että sivuilla on käytössä SSL-suojaus, jolloin osoite alkaa https-tekstillä ja selaimen alareunassa on lukko kiinni merkki.
- Käytä päivitettyä ja turvallista selainta.
- Jos viesti on epäilyttävä, tarkista lähettäjä puhelimitse.
- Asioi verkossa vain hyvämaineisten yritysten kanssa, jotka tiedät luotettavaksi.

(OnGuardOnline, 2011)

2.10 Laitteistojen vikasietoisuus

Vikasietoisuudella tarkoitetaan laitteiston kykyä toimia, vaikka se vikaantuisi. Tällainen vikasietoisuus edellyttää jonkinlaista taustalla toimivaa varmennusta. Vikasietoisuus koostuu kolmesta peruskäsitteestä: vikaantumisesta, viasta ja virheestä.

- Vikaantuminen on poikkeama laitteelle tai ohjelmalle tarkoitetusta oikeasta toiminnasta.
- Vika on laitteen tai ohjelman tila, joka voi aiheuttaa vikaantumisen.
- Virhe on laitteen tai ohjelman tuottama väärä toiminto, joka yleensä tarkoittaa sitä, että laiteta tai ohjelma on saanut väärän syötteen tai sitä on käytetty virheellisesti. Virhe voi myös johtaa järjestelmän vikaantumiseen.

Viat voidaan jakaa yleisiin vikamalleihin niiden keston-, näkymisen- ja vaikutuksen perusteella. Näitä vikamalleja ovat pysyvät viat, häilyvät viat, jotka vaativat korjausta mutta eivät vaikuta aina ja hetkelliset viat, jotka vaikuttavat mutta häviävät ilman korjausta.(Tiedonvälitystekniikka, 1998)

2.10.1 RAID

RAID(Redundant Array of Inexpensive Disks)-levyjärjestelmät ovat tapa lisätä kiintolevyjen vikasietoisuutta hajauttamalla tiedon tallentaminen usealle eri levylle. Tämä parantaa usein myös levyjärjestelmän suorituskykyä ja siitä on hyötyä konesalien lisäksi myös työasemakäytössä.(Vähimaa, 2009)

RAID-levyjärjestelmä parantaa vikasietoisuutta siinä vaiheessa kun levyrikko tapahtuu. RAID-kokoonpanosta riippuen yhtään tietoa ei välttämättä menetetä, eikä käytössä esiinny katkoa. Vikaantunut levy tulee vaihtaa silti mahdollisimman pian (Vähimaa, 2009). Alla on esitelty yleisimmin käytetyt RAID-kokoonpanot.

- RAID0 yhdistää käytössä olevat levyt yhdeksi tallennustilaksi, jolloin käyttöön saadaan kaikkien levyjen kirjoitusnopeus mutta jos yksikin levy hajoaa, menetetään kaikki data.
- RAID1 peilaa saman datan vähintään kahdelle eri levylle, jolloin data säilyy vaikka toinen levyista hajoaisi.
- RAID0+1 yhdistää edelliset tekniikat, joka parantaa nopeutta ja vikasietoisuutta.
- RAID5 tekniikassa käytetään datalevyjen lisäksi yhtä pariteettilevyä, jolloin mikä tahansa levy saa rikkoitua ja tiedot pystytään silti palauttamaan.
- RAID6 toimii kuten 5 mutta se käyttää enemmän pariteettidataa, jolloin kaksi levyä saa rikkoutua ennen kuin dataa menetetään.
- RAID10(1+0) yhdistää RAID0 ja 1 tekniikat jolloin, suorituskyky paranee levyjen mukaan mutta vain puolet levyistä on käytössä tallennusta varten, koska ne peilataan.

(Räty, 2005)

2.10.2 UPS ja kahdentaminen

UPS (Uninterruptible Power Supply) on laite, joka takaa katkeamattoman sähkönsyötön muille työympäristön sähkölaitteille. Laite kytketään pistorasian ja muun laitteiston väliin, jolloin UPS kykenee syöttämään sähköä tasaisesti, sekä pienten sähkökatkoksien ajan. UPS:ää ei ole tarkoitettu varavirtajärjestelmäksi pitkien sähkökatkoksien ajalle vaan sen tarkoitus on antaa riittävästi aikaa tärkeiden tietojen tallentamiseen ja koneen sulkemiseen sähkökatkoksen tullessa. (Japo, 2009)

UPS-laite sisältää yhden tai useampia akkuja, jotka takaavat sähkönsyötön muutamien minuuttien ajaksi sähkökatkoksen tapahtuessa. UPS-laitteet ovat hyvin yleisiä yrityksissä mutta niitä on tarjolla myös kotikäyttöön ja ovat erityisen hyödyllisiä jos kotona tehdään paljon etätyötä.(Japo, 2009)

Kahdentaminen on yleinen tapa lisätä tietojärjestelmän vikasietoisuutta. Kahdentamisella tarkoitetaan sitä, että esimerkiksi laitteesta, palvelimesta tai tietokannasta on käytössä koko ajan kaksi toisensa korvaavaa ja toisiaan tukevaa osaa, jolloin toisen hajotessa tai korruptoituessa toimintaa voidaan jatkaa vikaantumisesta huolimatta normaalisti. Kahdennus toteutetaan usein niin, että laite tai levyjärjestelmä sijaitsevat fyysisesti avain eri paikoissa. Tällä tavalla esimerkiksi tietylle alueelle kohdistuva uhka ei vaaranna saatavuutta.

3 Etätyö

Eurooppalaisen puitesopimuksen mukaan etätyö on työtä, jota tehdään säännöllisesti työnantajan tilojen ulkopuolella, vaikka työt voitaisiin tehdä myös työnantajan tiloissa. Lisäksi etätyössä edellytetään tietotekniikan hyväksikäyttöä joko työn tekemiseen tai organisointiin. Tämä ei kuintekaan sovi suomalaiseen työoikeuteen, joten sillä ei ole merkitystä työehtojen kannalta. Etätyöksi luetaan myös jokseenkin vakiintunut kotona tai muussa vastaavassa paikassa tehtävä etätyö, liikkuva etätyö ja työ etätyökeskuksissa. Etätyön puitesopimus ei sulje pois muitakaan etätyömuotoja, sillä tekniikan kehittyessä myös työmuodot muuttuvat. (Helle 2004, 41)

Yrittäjä voidaan lukea myös etätyön piiriin mikäli työtapa täyttää edellä mainittuja ominaispiirteitä. Tällaisilla yrittäjillä liiketoiminnan perustana voi olla esimerkiksi IT-alan asiantuntemus ja verkon käyttö myyntitarkoituksessa. (TE-Palvelut, 2008)

Yleisesti etätyöllä tarkoitetaan sitä, että työntekijä työskentelee kotonaan tai muussa valitsemassaan paikassa, joko kokonaan tai osittain. Etätyön tunnusomaisena piirteenä pidetään ajasta ja paikasta riippumattomia työjärjestelyjä. Etätyötä tekevä työntekijä valitsee etätyöpaikan yleensä itse sekä päättää työn alkamis- ja päättymisajat. (Helle 2004, 42)
Suuri osa etätyöntekijöistä tekee niin sanottua tietotyötä, joka kuvaa työn luonnetta ja etätyö työn järjestämisen tapaa. Tietotyössä työaika ja työpaikka sekä tietotekniikka ovat työn järjestelyn välineitä. (Pekkola 2002)

Yhä useampia työtehtäviä voidaan ainakin osittain suorittaa muualla kuin työnantajan tiloissa ja vuorokauden ajasta riippumatta. Kiinteästä työpaikasta ja työajasta kiinni pitäminen perustuu lähinnä perinteiseen tapaan ajatella työn organisointia. Etätyössä lähtökohtana on työn organisoiminen siten, että työ on tehokkainta sekä työnantajan että työntekijän kannalta. Yleisimmin etätyöpaikkana toimii työntekijän koti, mutta se voi olla lähes mikä tahansa muukin paikka. Usein puhutaan myös liikkuvasta etätyöstä tai mobiilista työstä, koska etätyötä tehdään myös työmatkoilla. Etätyöyhteyksien muodostamiseen käytetään matkapuhelinta ja kannettavaa tietokonetta, joilla yhteydet saadaan erilaisten erilaisten tietoliikenneyhteyksien avulla. (Helle 2004, 13)

Etätyö sopii parhaiten itsenäisiin työtehtäviin ja se on yleisintä ylempien toimihenkilöiden kohdalla. Etätyö vaatii organisaatiolta ennakkoluulottomuutta ja luottamusta työntekijöiden välillä sekä tietoteknisten edellytysten kunnossa oloa. Etätyö vaatii paljon myös työntekijältä itseltään. Haasteena ovat esimerkiksi työ- ja vapaa-ajan hämärtyminen ja sosiaalinen eristäytyminen työympäristöstä. Työnantajan kannalta suurimmat riskit liittyvät tietoturvallisuuteen ja työjärjestelyjen hallintaan. (Helle 2004, 14)

3.1 Etätyön puitesopimus

Etätyötä tehdään usein epävirallisesti, ilman kirjallista sopimusta, jolloin etätyöhön liittyvät asiat on sovittu hiljaisen sopimuksen perusteella tai työpaikan käytäntöön perustuen. Selvempien sääntöjen vuoksi Euroopan tasolla solmittiin etätyön puitesopimus vuonna 2002, jonka tarkoituksena pyrittiin luomaan yleiset ja yhteiset puitteet etätyölle. Suomessa puitesopimus otettiin käyttöön vuonna 2005. Etätyön puitesopimus tuo selkeyttä etätyön ehtoihin mutta työntekijän ja työnantajan välille jää edelleen paljon sovittavia asioita. Sovittavia asioita ovat ainakin työvälineet, kustannusten jako, työaika, työn johtaminen ja valvonta sekä yhteydenpito työpaikalle. (Helle 2004, 15)

Etätyön puitesopimus on EU maiden työmarkkinakeskusjärjestöjen välinen sopimus, jonka toteutuksesta vastaa maiden työmarkkinajärjestöt. Sopimusta ei kuitenkaan ole asetettu voimaan direktiivein, kuten monia muita Eurooppa-tason sopimuksia. Suomessa puitesopimuksessa mukana ovat valtion lisäksi palkansaajien- ja työnantajienkeskusjärjestöt, joten se kattaa laajasti suomalaisen työmarkkinakentän. (Helle 2004, 69)

Etätyön puitesopimus koostuu 12 otsikosta, joissa käydään läpi etätyön määritelmä ja tärkeimmät etätyössä huomioon otettavat asiat. Sopimus sisältää seuraavat otsikot:

- Yleiset näkökohdat
- Etätyön määritelmä
- Etätyön luonne
- Työsuhteen ehdot
- Tietoturva
- Yksityisyyden suoja
- Työvälineet
- Työsuojelu
- Työjärjestelyt
- Koulutus
- Kollektiivisia oikeuksia koskevat kysymykset
- Täytäntöönpano ja seuranta

3.2 Etätyö Suomessa

Etätyöllä on Suomessa jokseenkin vakiintunut merkitys mutta sillä ei ole olemassa virallista määritelmää työlainsäädännössä. Etätyö luetaan normaaliksi tavaksi tehdä työsuhteista työtä, kuten esimerkiksi tiimityö, minkä vuoksi ei ole tarvetta etätyöntekijän juridiselle määrittelylle. (Helle 2004, 42)

Etätyöstä käytetään usein eri termejä, joilla halutaan tarkentaa etätyön kuvaa. Tietotekniseen etätyöhön viitataan usein termillä e-työ (electronic work), jolla tarkoitetaan työtä tietoverkoissa. Etätyön katsotaan olevan osa laajempaa käsitettä ja e-työ onkin osittain korvannut etätyö-termin työelämässä. (Pekkola 2002)

EU:ssa tietotekniikan hyväksikäyttö on vakiintunut osaksi etätyön määritelmää, joka ilmenee esimerkiksi puitesopimuksessa olevasta vaatimuksesta. Suomessa tietotekniikan hyväksikäyttöä ei kuitenkaa edellytetä. Tosin käytännössä tietotekniikkaa käytetään enemmän tai vähemmän etätyönteossa, riippuen työtehtävistä, mutta Suomessa sitä ei ole haluttu sitoa vain tiettyyn työvälineeseen. (Helle 2004, 45)

3.3 Etätyömuodot ja paikat

Etätyömuodot kehittyvät jatkuvasti tietotekniikan ja tietoliikenneyhteyksien mukana. Sen vuoksi virallista jaottelua etätyömuodoista ei ole olemassa. Etätyömuodolla ei ole vaikutusta työntekijän asemaan, jolloin työmuodon valintaan vaikuttavat työntekijän ja työnantajan tarpeet sekä käytettävissä olevat ratkaisut. Nopean kehityksen vuoksi etätyön puitesopimuskaan ei määrittele etätyön eri muotoja. (Helle 2004, 49)

Etätyömuotoja erotellaan, jotta saadaan parempi kuva etätyön eri mahdollisuuksista. On olemassa useita eri jaotteluja mutta yleisimmiksi etätyömuodoiksi voidaan lajitella ainakin seuraavat:

- Kotona tai muussa työntekijän valitsemassa paikkassa tehtävä etätyö.
- Etätyökeskuksessa tehtävä etätyö, jossa jaetut toimistotilat.
- Liikkuva etätyö.
- Yrittäjänä tehtävä etätyö.

(Helle 2004, 49-53)

Yleisin etätyömuoto on työntekijän kotona tai muussa valitsemassa paikassa tekemä etätyö. Etätyöpaikkana voi tällöin olla esimerkiksi kesämökki tai hotelli. Useinmiten kotona työskentelevällä etätyöntekijällä olisi myös paikka työnantajan toimistolla. (Helle 2004, 50)

Etätyökeskuksissa tehtävä etätyö on harvinaisempaa kuin kotona. Tällaisessa työmuodossa etätyöntekijä työskentelee erillisissä toimitiloissa muiden etätyöntekijöiden kanssa. Yleensä tätä muotoa käytettäessä työnantajan toimitilat sijaitsevat kaukana eri paikkakunnalla, eikä työntekijä halua tehdä työtä itsekseen kotona. Tämän työmuodon etuna on työyhteisön läsnäolo ja työrauha, joka saattaa kotoa puuttua. (Helle 2004, 51)

Yrityksillä on mahdollista vuokrata etätyötiloja, jolloin tapaamiset ja kokoukset ovat helposti järjestettävissä ilman omia tiloja ja yhteyksiä. Usein etätyöpisteen vaatimuksena on internet-yhteyksen saaminen, joka on yksi tärkeimmistä kriteereistä etätyön mahdollistamiselle ylipäänsä. Etätyöpisteeseen eduksi voi laskea myös sen että sinne voi sopia samalle päivälle useita tapaamisia sen sijaan, että kiertäisi ympäri kaupunkia eri paikoissa. (Petrasol, 2009)

Eurooppalaisissa tutkimuksissa liikkuvaksi etätyöksi määritellään työ, jota tehdään vähintään 10 tuntia viikossa siellä, missä satutaan liikkumaan ja ollaan yhteydessä työnantajaan ja asiakkaisiin mobiiliyhteyksien avulla. Liikkuva etätyö lisääntyy jatkuvasti matkustamisen ja parantuneiden mobiiliyhteyksien myötä (Helle 2004, 53). Liikkuvan etätyön tyypillisimpiä etätyöpaikkoja ovat asiakkaan luona, hotellissa tai lentoasemalla. Liikkuvat etätyöpaikat voivat vaihdella paljon ja niitä voivat olla myös julkiset kulkuvälineet kuten bussi, juna tai lentokone (Helle 2004, 126)

Yrittäjänä työskentelevä etätyöntekijä on yleensä freelancer tai ammatinharjoittaja, joka työskentelee kotitoimistossaan ja käyttää tietoliikennetekniikkaa yhteydenpidossa asiakkaiden ja muiden yhteistyökumppaneiden kanssa. Tätä etätyömuotoa käyttävät esimerkiksi juornalistit ja konsultit. (Helle 2004, 54)

Etätyömuodot kertovat suurin piirtein työssä käytettävät etätyöpaikat. Etätyöntekemispaikka on hyvä määritellä etätyösopimuksessa. Sopimuksen lisäksi työntekijän ja työnantajan on syytä sopia mitä reunaehtoja etätyön tekemiseen eri paikoissa liittyy. Etätyöntekijällä tulee olla työntekoon käytettävä rauhallinen työtila. Esimerkiksi kotona tehtävä etätyö epäonnistuu helposti jos häiriötekijöitä on ympärillä. Tutkimusten mukaan etätyönteon olosuhteet vaikuttavat merkittävästi työn laatuun ja työntekijän tyytyväisyyteen. (Helle 2004, 126)

3.4 Etätyön hyödyt ja riskit

Alun perin etätyön käsite on kehitelty Kaliforniassa Yhdysvalloissa, jossa haluttiin vähentää työmatkaliikennettä ja säästää länsi-rannikon kalliissa toimistotiloissa. Suomessa varsinkin pääkaupunkiseudulla ruuhkat kasvavat jatkuvasti, jolloin ajalliset kilometrit ovat erittäin pitkiä. Pääkaupunkiseudun tilanne suosii erityisesti etätyön työmuotoa. Työmatkaan kuluvan ajan hyötykäyttö onkin tärkeä peruste etätyöhön siirtymisessä Suomessa. Etätyöhön siirrytään yleensä silloin kun siitä hyötyy sekä työntekijä että työnantaja. Vaikka riskejä onkin olemassa molemmin puolin, niitä voidaan vähentää hyvällä ennakkosuunnittelulla ja sopimalla asioista etukäteen. (Helle 2004, 16)

”Elisa Oyj kertoo, että virtuaaliset verkkokokoukset ja etätyö ovat tuoneet yritykselle jättimäisiä säästöjä. Elisa laskee säästäneensä pelkästään vuoden 2009 viitenä kuukautena kaksi miljoonaa euroa. Säästyneiden matkojen määrä on melkoinen, mikä tietää myös ympäristösäästöjä.” (Kotilainen, 2009)

3.4.1 Työntekijän näkökulma

Ehdotus etätyöstä tulee yleensä työntekijältä, sillä etätyössä on etätyöntekijälle monia etuja. Työntekijän arvostamia etuja ovat esimerkiksi: työajan järjestely, työrauha, mahdollisuus yhdistää työ ja vapaa-aika, työmatkojen ja matkakustannuksien väheneminen ja vapaa-ajan lisääntyminen. (Helle 2004, 17)

Yleensä etätyössä on mahdollista määritellä omat työskentelyajat. Monet ihmiset eivät tykkää 8-16 työskentelystä, jolloin töitä voidaan tehdä silloin kun itselle parhaiten sopii. Perhe-elämään ja harrastuksiin liittyvät syyt puoltavat etätyön puolesta, sillä joustavuutta löytyy päivittäisten toimien järjestelyyn löytyy huomattavasti enemmän. Työmatkaan voi pääkaupunkiseudulla kulua jopa useampi tunti päivässä. Työmatkojen jäädessä vähäisiksi, etätyöntekijälle kertyy merkittävät säästöt sekä taloudellisesti että ajallisesti. Edellä mainitut tekijät lisäävät esimerkiksi työtyytyväisyyttä, motivaatiota, yöunta ja vapaa-aikaa. (Helle 2004, 18-19)

Etätyöhön liittyvillä eduilla on myös kääntöpuolia, jotka voivat muodostua etätyöntekijöiden haitaksi. Näitä haittoja voivat olla esimerkiksi: työyhteisön puute, liiallinen työmäärä, urakehityksestä sivuuttaminen, ongelmat teknisessä toteutuksessa ja työsuojelupuutteet. Kokoaikaisella etätyöntekijällä työn puolesta tulevat sosiaaliset kontaktit saattavat jäädä todella vähiin, jolloin seurauksena voi olla eristäytyminen työyhteisöstä. On myös mahdollista että työskentelystä kotona ei tule mitään kun työ ja vapaa-aika sekoittuvat. Valvovan silmän poissaollessa etätyöntekijä voi kärsiä esimerkiksi ergonomisen työasennon puuttumisesta tai jäädä jopa urakehityksestä sivuun. Myös töitä saatetaan sysätä etätyöntekijän niskaan tietämättä koituvista ylitöistä ja stressistä. (Helle 2004, 20-21)

3.4.2 Työnantajan näkökulma

Merkittävimpiä etuja työnantajalle ovat esimerkiksi: työn tehokkuuden ja joustavuuden paraneminen, organisoinnin kehittyminen, työhyvinvoinnin lisääntyminen, kustannussäästöt, houkuttelevuus työnantajana ja imagoarvo ympäristöasioissa. Useista tutkimuksista on käynyt ilmi, että etätyönä tehty työ on tehokkaampaa ja joustavampaa, koska työntekijä pystyy tekemään omat järjestelynsä olosuhteiden ja vireystilansa suhteen. Etätyön asianmukainen hallitseminen parantaa yrityksen organisointia, houkuttelevuutta ja imagoarvoa. Nämä ovat erittäin merkittäviä uusien työntekijöiden rekrytoinnissa ja yrityksen ulkoisessa kuvassa. Kustannussäästöjä syntyy, kun yritys ei tarvitse niin suuria toimistotiloja. Vaikka etätyö olisikin osittaista, säästöjä saadaan silti luopumalla työntekijöiden omista työpisteistä ja kiinteistä työasemista. (Helle 2004, 22-24)

Työnantaijan kannalta etätyön huonoja puolia ovat esimerkiksi: kustannusten lisääntyminen, tietoturvallisuusriskit, työjärjestelyjen hallinta, työntekijöiden valvonta sekä tiedonhallinta ja hiljaisen tiedon välittyminen. Kustanuksia kertyy tarvittavan laitteiston ja työvälineiden hankkimisesta. Tietoturvallisuus maksaa myös ja on usein heikompi kuin yrityksen tiloissa. Työjärjestelyjä, työntekijää ja tiedonhallintaa on huomattavasti vaikeampi valvoa, kun työntekijään ei ole visuaalista kontaktia. Työpaikoilla tärkeä niin sanottu hiljaisen tiedon välittyminen ja kollegojen opastus saattaa puuttua etätyön vuoksi. Etätyö haittaa myös mahdolista tiimityötä, jota on vaikeampaa järjestää etätyöntekijöiden kesken. (Helle 2004, 25-27)

3.5 Tietoturvallisuus etätyössä

Tietoturvallisuudella tarkoitetaan sitä, että kukaan ulkopuolinen ei pääse käsiksi sellaisiin tietoihin, joihin hänellä ei ole lupaa. Tietoturvallisuus voidaan määritellä myös turvallisuuden osa-alueeksi, joka käsittelee tietoriskejä ja tietojenkäsittelyä. Etätyön tietoturvallisuus on haaste sekä työntekijälle että työnantajalle, koska etätyössä tietoturvariskit lisääntyvät normaaliin toimistotyöhön verrattuna. Tietoturvallisuus on usein työnantajan kannalta merkittävä este etätyönteolle, koska tiettyjen työtehtävien ja tietojen käsittelyn vaatima tietoturvataso ei toteudu. Vastuu tietoturvallisuuden järjestämisestä on työnantajalla mutta tietoturvallisuuteen vaikuttaa paljon myös työntekijän toimintatavat. Tärkeää on, että tietoturvallisuusriskeihin on varauduttu etukäteen ja toimintatavat on kerrottu selkeästi kaikille osapuolille. Tietoturvallisuus perustuu pitkälti työpaikoissa sisäisesti määriteltyihin sääntöihin ja tietoturvallisuusohjeisiin. (Helle 2004, 191)

3.5.1 Vastuu tietoturvasta

Työnantaja vastaa tietoturvallisuuden järjestämisestä mutta myös työntekijän toimintatavat ovat tärkeässä osassa tietojen turvaamisessa. Tietoturvallisuuden säännöksiä on sisällytetty eri lakeihin, eikä yhtenäistä tietoturvallisuuslainsäädäntöä Suomessa ole. Työnantaja vastaa tietoturvallisuuden ylläpidon aiheuttamista kustannuksista, koska työnantajan intressinä on yritystä ja työntekijöitä koskevien tietojen salassapysyminen. (Helle 2004, 192)

Aiemmin tässä työssä mainittu etätyön puitesopimus sisältää määräykset etätyön tietoturvallisuudesta ja vaatimuksista. Puitesopimuksen mukaan työnantaja valitsee ne keinot, joita tiedon turvaamiseksi käytetään. Valitut keinot riippuvat työn luonteesta, tietojen tärkeydestä, käytettävistä laitteista ja tiedonsiirtoyhteyksistä. Puitesopimus koskee etätyöntekijän ammatillisiin tarkoituksiin käyttämän tiedon suojausta, jolloin työnantaja ei ole vastuussa työntekijän henkilökohtaisiin asioihin liittyvistä tiedoista. (Helle 2004, 192)

Etätyön puitesopimuksen mukaan työnantajan on annettava työntekijälle tiedot tietoturvallisuutta koskevasta lainsäädännöstä ja yrityksen omista säännöistä. Säännöillä tarkoitetaan esimerkiksi salasanoja ja niiden käsittelyä. Työntekijän velvollisuus on noudattaa kaikkia tietoturvallisuuteen liittyviä työnantajan antamia ohjeita. Työnantajan vastuulla on etätyön vaatimien työvälineiden, kuten tietokoneen, sähköpostin ja tiedonsiirtoyhteyksien hankinta. Tämän jälkeen työnantajan tulee tiedottaa mahdollisista rajoituksista työvälineiden käytön suhteen. Tämä koskee esimerkiksi laitteiston käyttämistä työntekijän henkilökohtaisia tarkoituksia varten tai internetin käyttöön liittyviä rajoituksia. Työnantajan on tiedotettava työntekijälle mahdollisista seuraamuksista, joita sääntöjen laiminlyönnistä aiheutuu. Tietoturvallisuuden laiminlyönnistä aiheutuvat seuraukset kohdistuvat aina työnantajaan itseensä, mikä tarkoittaa sitä, että tietoturvallisuudesta huolehtiminen ei voi olla etätyöntekijän vastuulla, vain työnantaja ohjeiden mukaan toimiminen. (Helle 2004, 194)

3.6 Etäyhteydet ja laitteet

Etätyön tekemisen edellytyksenä on toimiva tietoliikenneyhteys etätyöpisteestä yrityksen verkkoon. Yhteydeksi on usein tarjolla eri vaihtoehtoja, joita esitellään seuraavaksi. Yhteyksiä voidaan hyödyntää monilla eri laitteilla, jotka usein ovat kannettavia tai muuten helposti liikuteltavia.

Tietoa voidaan välittää ilman, että ollaan esimerkiksi sisätiloissa tai langallisesti kiinni verkossa. Keskeinen ominaisuus paikasta riippumattomalle yhteydenpidolle on myös realiaikaisuus. Tieto liikkuu nopeasti paikasta toiseen, joka mahdollistaa nopean kommunikoinnin verkon välityksellä (Lepistö, 2002).

3.6.1 Mobiiliyhteydet

Mobiiliyhteydellä tarkoitetaan fyysisesti hyvin vapaasti liikuteltavaa yhteyttä verkkoon. Liikuteltava mobiiliyhteys voidaan muodostaa mobiililaitteella, kuten kannettavalla tietokoneella, tabletilla tai matkapuhelimella (Vartiainen, 2005).

Mobiiliyhteyden käyttöpaikkoja ovat yleensä esimerkiksi jokin uusi työpiste tai rakennus, kulkuväline ja toinen paikkakunta. Mobiiliyhteyden fyysisellä paikalla on erilaisia ominaisuuksia. Paikan etäisyys voi vaihdella ja niitä voi olla yksi tai useita. Fyysinen paikka voi myös olla itse liikkuva kuten esimerkiksi bussi, juna ja lentokone (Vartiainen, 2005).

Mobiiliyhteydet käyttävät yhteystekniikkana langattomia yhteyksiä, joista yleisimpia ovat WLAN, Edge, Gprs, 3G ja 4G. WLAN yhteydet ovat yleisiä kiinteissä etätyöpisteissä, joissa voidaan päästä n. 100Mbit/s nopeuksiin. Yleisin vaihtoehto nykyään on lähes jokaisesta älypuhelimesta löytyvä 3G yhteys, jolla päästään parhaimmillaan 10-20Mbit/s nopeuksiin. Älypuhelimesta yhteys voidaan jakaa käyttämällä puhelinta WLAN-jakajana, jolloin yhteys on minkä tahansa kannettavan laitteen käytössä, josta löytyy WLAN. (Berschewsky, 2012)

3.6.2 Mobiililaitteet

Mobiililaitteesta puhuttaessa tarkoitetaan laitetta, joka on kompaktin kokoinen ja helppo kuljettaa mukana. Sillä on yhteyksien salliessa mahdollista lähettää ja vastaanottaa tietoa paikasta riippumatta. Mobiililaitteella voidaan myös olla yhteydessä muihin verkossa oleviin laitteisiin (Lepistö, 2002).

Mobiliilaitteelle ominaisia piirteitä ovat: verkottuneisuus, globaalisuus, kompakti koko, reaaliaikaisuus ja interaktiivisuus. Nämä piirteet täyttäviä yleisemmin käytettyjä laitteita ovat esimerkiksi kannettava tietokone, matkapuhelin, tablet, PDA-laite ja kämmentietokone (Lepistö, 2002).

3.6.3 VPN-yhteys

VPN (Virtual Private Network) on tekniikka, jolla voidaan luoda virtuaalinen yksityisverkko määriteltyjen pisteiden välille. VPN-yhteys käyttää hyödyksi tarjolla olevia verkkoja, joita pitkin se luo oman yksityisen yhteyden käyttäen tunnelointiprotokollaa. Yhteys toimii tämän jälkeen samaan tapaan kuin käyttäjä olisi suoraan kiinni yrityksen verkossa. Käyttäjällä on pääsy samoihin sisäverkon palveluihin, kuten intranetiin ja verkkolevyille. (VPN Consortium, 2008)

Yhteys voidaan luoda esimerkiksi kahden verkon välille tai etäyhteydeksi yksittäisestä työasemasta yrityksen verkkoon. Verkkojen välinen VPN-yhteys voidaan toteuttaa reitittimestä reitittimeen tai yhteydelle voidaan määritellä erillinen kone valvomaan ja hallinnoimaan VPN-liikennettä.(Microsoft Technet, 2001)

VPN-yhteyden muodostaminen yksittäiseltä työasemalta tapahtuu siten, että työasema lähetää paketin, jolla se todentaa itsensä palvelimelle ja palvelin todentaa itsensä takaisin. Salattua tietoa ei pysty purkamaan ilman avainta, jolla yhteys on salattu. VPN-yhtes toteutetaan tunnelointiprotokollan avulla, joissa on omat tekniikkansa myös yhteyden salaukseen. Tähän tarkoitettuja standardeja ovat: Ipsec, L2TP, L2F ja PPTP protokollat. (Microsoft Technet, 2001)

4 Etätyön tietoturvaohje

Yritykselle tarvitaan ohjeistus, josta löytyy koottuna etätyön tietoturvassa huomioon otettavat osa-alueet. Tässä etätyön tietoturvaohjeistuksessa käydään läpi kuinka olemassa olevia riskejä pystytään kullakin osa-alueella välttämään. Ohjeistus perustuu valtiovarainministeriön etätyöntietoturvaohjeistuksessa (Vahti 3/2002) ja valtion tietoturvallisuussuosituksessa (VM 1/1999) määriteltyihin tietoturvallisuuden osa-alueisiin, joita täydentää tämän työn teoriaosuuden aineisto sekä kansallinen turvallisuusauditointikriteeristö (KATAKRI 2011).

Etätyön tietoturvallisuus vaatii panostusta sekä työntekijältä, että työnantajalta. Työnantajan tulee huolehtia teknisistä järjestelyistä ja työntekijän tarvitsemista palveluista. Työntekijä huolehtii puolestaan vastuullisesta, tietoturvallisuuden huomioon ottavasta työtavasta. (VM 2002)

4.1 Tietoliikenneturvallisuus

Tietoliikenteen turvaaminen on erittäin tärkeää tietoteknisessä toiminnassa, jota tehdään tietoverkkojen välillä. Etätyössä kyseessä on yleensä etätyöpisteen ja yrityksen verkon välinen yhteys. Turvallinen yhteys yrityksen verkkoon voidaan taata käyttäjän tunnistautumisella ja yhteyden salaamisella. Tähän on olemassa useita ratkaisuja, joista yleisin on VPN(Virtual Private Network) yhteys. VPN yhteydellä käyttäjä tunnistautuu muuttuvan koodin avulla ja luo sen jälkeen salatun yhteyden yrityksen verkkoon, joka toimii sen jälkeen samalla tavalla kuin käyttäjä olisi suoraan kiinni yrityksen verkossa.

Huomiota kannattaa kiinnittää myös siihen mikä yhteys työntekijällä on käytössä ja kuinka turvallinen se on. Esimerkiksi kaikille avoimet WLAN verkot eivät ole suositeltuja yhteystapoja kun puhutaan työntekoon käytettävästä tietoliikenneturvallisesta yhteydestä.

Yleisimmät työntekoon käytettävät yhteydet voidaan jakaa kahteen osaa. Kiinteä yhteys ja mobiili yhteys. Etätyössä kiinteä yhteys on yleisin kotoa tapahtuvassa työssä, jolloin turvallisuuden näkökulmasta tärkeää on oman yhteyden ja laitteiston salaus niin, ettei niihin päästä käsiksi ulkopuolelta. Etätyössä käytettävistä mobiiliyhteyksistä yleisimmät tekniikat ovat 3G, 4G ja WLAN. Nämä ovat yleisiä myös kotikäytössä mutta erityistä huomiota tulee kiinnittää etätyössä usein käytettyihin julkisesti tarjolla oleviin yhteyksiin, jolloin samaa yhteyttä käyttää useat eri henkilöt ja ilman yhteyden salausta liikennettä voidaan seurata. Salattu yhteys tulee tässä tapauksessa avata heti yhteyden auettua, ennen kuin työasioita aletaan käsittelemään tai kirjaudutaan yrityksen järjestelmiin. Tietokoneessa tulee olla aktiivinen palomuuri, joka estää ulkopuolisten pääsyn koneelle avoimen verkon kautta.

4.2 Laitteistoturvallisuus

Etätyössä käytettävät laitteet tulee olla työnantajan hallitsemia ja hyväksymiä, jotta voidaan taata niiden tietoturvallisuus. Laitteiston sisäänrakennetut ja asennetut tietoturvaratkaisut on oltava käytössä aina kun ollaan tekemisissä työhön liittyvän materiaalin kanssa. Näin varmistetaan, että laitteistolle määritelty perustason tietoturva on käytössä jokaisen työntekijän kohdalla.

Vikatilanteissa laitteiston huolto tulee aina suorittaa yrityksen toimintamallin mukaan, jolloin asiasta ilmoitetaan sille taholle, joka laitteista vastaa ja huoltoprosessi voidaan käynnistää yrityksen käytännön mukaisesti. Sama taho vastaa yleensä myös teknisestä tuesta. Uusien laitteiden hankinnasta vastaa mahdollisuuksien mukaan aina yrityksen määrittämä taho, jolloin laitekanta on helpommin hallittavissa, eikä turhia tietoturvaa heikentäviä poikkeuksia pääse syntymään.

Etätyölaitteet tulee olla turvamerkittyjä erityisesti matkapuhelinten, tabletien ja kannettavien tietokoneiden osalta, jolloin varkaustilanteessa anastetun laitteen käyttö ja jälleenmyynti vaikeutuu sekä löytötavaran palauttaminen omistajalleen helpottuu.

Tärkeimmät tietoaineistoa sisältävät laitteet kuten palvelimet ja levyjärjestelmät tulee olla varmistettuja varavirtalähteiden sekä varmuuskopioiden avulla. Nämä voidaan toteuttaa esimerkiksi UPS laitteella ja kahdentamalla järjestelmät.

4.3 Tietoaineistoturvallisuus

Etätyön tietoaineistosta puhuttaessa aineisto rajataan tietoihin, jotka sisältää yritystä tai sen toimintaa koskevia tietoja. Näiden tietojen paljastuminen on suuri riski, joka on otettava huomioon tietoturvallisessa tietojenkäsittelyssä.

Tietoaineistoturvallisuuden perustaso voidaan taata noudattamalla rutiininomaisesti tiettyjä toimintamalleja. Alla on lueteltuna toimenpiteet, joita noudattamalla tietoaineiston perustason turvallisuus on aina olemassa.

- Tietoaineiston tuhoaminen määritetyllä tavalla
- Tiedonkäsittely tietoaineistolle luokitetulla tavalla
- Tietojen varmuuskopiointi
- Tiedostojen salaus

Luokitellun tietoaineiston hävittäminen tulee suorittaa ensisijaisesti työpaikalla työnantajan toimesta. Luokiteltu paperiaineisto voidaan tuhota silppurilla ja toimituksella uusiokäyttöön. Kiintolevyt ylikirjoitetaan siihen tarkoitetuilla sovelluksilla tai tuhotaan demagnetointilaitteilla.

Etätyössä tulee varmistaa tiedostojen varmuuskopiointimahdollisuus. Tämä olisi hyvä käydä suorittamassa säännöllisesti yrityksen omassa verkossa siihen tarkoitettujen sovellusten avulla. Mikäli tämä ei ole mahdollista, tulee työntekijän hoitaa varmuuskopiointi itse ja salattava kopioitu tietoaineisto.

Yritystä koskevan materiaalin lähettäminen julkisen verkon yli salaamattomana ei ole suositeltavaa vaan sähköpostiliikenne tulee olla salattua. Salauksen voi tehdä käyttämällä vähintään salattua yhteyttä, jonka lisäksi tarjolla on sovellusten omat salaustoiminnot, joilla liitetiedostot voi salata. Koko viestin salaamin on mahdollista erilaisilla sovelluksilla kuten esimerkiksi PGP:llä.

4.4 Ohjelmistoturvallisuus

Tietoturvallisen työskentelyn varmistamiseksi, niin normaalissa toimistotyössä, kuten myös etäkäytössä vaadittavia sovelluksia ovat virustorjunta ja palomuuri. Näillä voidaan suojautua suurimmalta osalta vahingollisia haittaohjelmia, joita verkossa liikkuu. Virustorjunnasta tulee ohjeistaa työntekijöitä riittävästi ja kaikista havainnoista tai tartunnoista on ilmoitettava tietoturvasta vastaavalle taholle. Virustorjunnan lisäksi tulee käyttää määriteltyä ohjelmistoa tiedostojen ja liikenteen salaukseen.

Ohjelmistojen asennuksista tulee vastata sille määritelty taho, joka suurimmassa osassa yrityksistä on tietohallinto. Ohjelmistojen pääsynvalvonta tulee toteuttaa normaalin käyttäjätunnus/salasana menettelyn mukaisesti.

Käyttäjien oikeuksia tulee hallita keskitetysti, jotta työntekijät eivät pääse asentamaan ohjelmia oman mielensä mukaan ja vaarantamaan tietoturvaa mahdollisilla haittaohjelmien lataamisella.

Käyttöjärjestelmien automaattiset päivitykset tulee olla aina päällä ja ne on asennettava julkaisun jälkeen mahdollisimman pian, jotta löydetyt haavoittuvuudet korjaantuu ja päivitykset ovat aina ajan tasalla.

4.5 Käyttöturvallisuus

Työntekoon tarvittavat materiaalit halutaan yleensä olevan saatavilla myös etätyötä tehtäessä, mikä asettaa suuria haasteita tietoturvan säilyttämisen kannalta. Työssä käytettävä aineisto on usein sellaista, jonka ei haluta missään nimessä joutuvan ulkopuolisten käsiin. Sen vuoksi käyttöoikeudet tulee olla vain sellaisilla henkilöillä, jotka tietoja tarvitsevat ja joilla on oikeus käyttää tietoja.

Etätyössä on erittäin tärkeää, että käyttäjä tunnistautuu ja tunnistautuminen pystytään todentamaan. Tämä voidaan toteuttaa tietoturvallisesti vahvalla käyttäjätunnuksella ja salasanalla, jolloin käytetään joukkoa sattumanvaraisia merkkejä sekä lisäksi erilaisilla muuttuvan salasanankäytön tekniikoilla. Tällainen kertakäyttösalasana on hyvin yleinen, luotettava ja myös helppokäyttöinen, sillä usein riittää kun tunnistautuu istunnon alussa.

Järjestelmän pääsynvalvonnalla valvotaan sitä, ketkä järjestelmään kirjautuvat ja näin voidaan myös seurata ulkopuolisia tunkeutumisyrityksiä. Pääsynvalvonta voidaan toteuttaa monin eri tekniikoin mutta yleisesti toiminta perustuu pääsynvalvontalistoihin, joilta järjestelmä tarkistaa käyttöoikeudet. Pääsynvalvontalistoille voidaan määritellä erikseen käyttäjän oikeudet esimerkiksi tunnuksen, IP-osoitteen tai jonkun muun tiedon avulla.

Kaikista ohjelmiin ja tietojärjestelmiin kirjautumisista tulee säilyttää tietosuojasäännösten puitteissa lokitiedosto, jolloin voidaan tutkia mahdollisia tunkeutumisyrityksiä jälkeenpäin.

4.6 Luokitellun tiedon käsittely

Yrityksen kannalta tärkeäksi luokiteltua tietoa tulee käsitellä huolellisesti, ettei se päädy ulkopuolisten haltuun. Vaikka etätyötä tehtäisiin omassa kodissa, voivat tiedot päätyä ulkopuolisten käsiin huomattavasti helpommin kuin työnantajan tiloissa.

Jokaiseen etätyöympäristöön tulee miettiä kuinka niissä toimitaan ja tarvittaessa soveltaa annettua ohjeistusta. Erityistä huomiota tulee kiinnittää työhön liittyvän aineiston hävittäminen ja työssä syntyvän aineiston arkistointiin.

Tietojen ja tiedostojen luokittelulla määritellään, kuinka niiden kanssa tulee toimia. Määrittely voidaan tehdä suojaustasojen mukaan. Mitä tärkeämpää tietoaineisto on, sitä tarkemmin aineistoa tulee käsitellä ja sitä korkeampi suojaustaso tiedoilla on.

Luokiteltu tietoaineisto voi olla sellaista, että sitä saa käsitellä vain työnantajan tiloissa, joissa liikkuvat henkilöt voidaan tunnistaa. Tämä estää usein etätyön tekemisen kokonaan. Luokittelu vaikuttaa myös asiakirjojen käsittelyyn ja siirtämiseen sähköisesti. Nämä ovat yleensä sallittuja vain sellaisissa tietojärjestelmissä ja verkoissa, joiden turvallisuus voidaan taata.

4.7 Hallinnollinen turvallisuus

Hallinnollisesta turvallisuudesta vastaa yrityksen tietohallinto tai siihen määritelty muu erillinen taho. Tämän tahon tehtävänä on toteuttaa yrityksen tietoturvamäärityksiä ja varmistaa, että tietoturvallinen työskentely on mahdollista myös työpaikan ulkopuolella. Etätyön kannalta tärkeimpänä pidetään etätyöpisteen ja yrityksen välistä tietoliikennettä ja sen tietoturvallisuutta.

Etätyöntekijälle on tarjottava tarvittava tuki niin tietojenkäsittelyyn kuin tietojärjestelmien käyttöön. Tietohallinto valvoo järjestelmien etäkäyttöä ja yhteyksiä. Mikäli puutteita esiintyy, niistä raportoidaan välittömästi eteenpäin. Valvontamenettely tulee olla myös työntekijän tiedossa. Tarvittaessa on järjestettävä koulutusta ja opetusta, jotta työntekijä tietää mitä toimia ja järjestelmiä seurataan.

Tietohallinto haliitsee työntekijän käyttämiä laitteita, yhteyksiä, tunnuksia ja tietoaineistoja. Etätyön päätyttyä hallinnon tulee pitää huoli siitä, että kaikki palautuu takaisin yritykselle ja tarpeeton työntekijään liittyvä aineisto, kuten tunnukset ja oikeudet poistetaan.

5 Työn arviointi ja jatkotutkimukset

Opinnäytetyöni onnistui mielestäni hyvin ja uskon, että siitä on hyötyä ainakin tietoturvaan perehtymättömille Proact Finland Oy:n työntekijöille. Työssä pyrittiin etenemään konstruktiivisen tutkimuksen vaiheiden mukaan. Vaiheet ohjasivat työtä jouhevasti eteenpäin ja niiden mukaisesti pyrin etenemään.

Työ on jaettu periaatteessa neljään osaan. Aluksi johdatellaan työn sisään ja kerrotaan mitä on aiemmin tehty ja miksi tähän työhön on päädytty. Johdannosta käy ilmi myös mitä työllä tavoitellaan ja miten työ on tehty. Teoriaosuuteen on luotu kaksi toisistaan selkeästi eriävää osaa, johtuen aiheesta. Työ yhdistää etätyön ja tietoturvan, joten tämä oli mielestäni hyvin looginen ratkaisu.

Teoriaosuuden pohjalta etätyön tietoturvaohjeistuksen luominen oli hyvä tehdä. Mielestäni teoriaosuus on sopivan laaja ja yksityiskohtainen, jonka pohjalta ohjeistus voidaan tehdä. Otin huomioon myös sen, että aineisto, sekä ohjeistus tulevat normaalien työntekijöiden käyttöön, jotka eivät ole IT-alan ammattilaisia. Tämän vuoksi varsinkin ohjeistus on pyritty pitämään tarpeeksi yksinkertaisena.

Työlle on mielestäni paljon mahdollisia jatkotutkimuksen aiheita niin etätyön kuin tietoturvankin puolesta. Tietoturva on todella laaja käsite, jossa voidaan syventyä tarkemmin esimerkiksi johonkin tiettyyn tietoturvan osa-alueeseen. Proact toimii erilaisten tallennusratkaisujen asiantuntijayrityksenä, jolloin hyviä jatkotutkimuksen aiheita voisivat olla tietoliikenneturvallisuus ja tietoaineistoturvallisuus.

Jatkotutkimuksissa voitaisiin siirtyä yksittäisen työntekijän näkökulmasta kokonaisen yrityksen mittakaavaan, jolloin olisi mahdollista tarjota asiakkaille uusia palveluja näiden tutkimuksien perusteella.

Etätyön tekeminen lisääntyy ja kehittyy jatkuvasti parantuvien yhteyksien puolesta. Yhteydet nopeutuvat ja ovat päivä päivältä laajemmin saatavilla. Mahdolliset jatkotutkimukset voisivat liittyä uusiin yhteysnopeuksiin ja yhteyden saatavuuteen eri puolilla Suomea tai jopa ulkomailla.

Lähteet

Berschewsky, T. 2012. Kotiverkko kuntoon. Viitattu: 2.5.2013.
http://www.mbnet.fi/artikkeli/lehti/nettijatkot/nettijatko_kotiverkko_kuntoon

Cert-Fi, 2007. Suojautuminen Phishing hyökkäyksiltä. Viitattu: 12.10.2012.
http://www.cert.fi/ohjeet/2005/ohje-2005-01.html

Datta, G. 2012. What are Trojans?. Viitattu: 10.4.2013
http://securaid.com/index.php/windows/trojans

Datta, G. 2012. What is Spyware? Viitattu: 11.4.2013
http://securaid.com/index.php/windows/spyware

Etätyön puitesopimus, 2002. Etätyötä koskeva puitesopimus. Viitattu: 15.12.2012.
http://www.akava.fi/files/465/Etatyon_puitesopimus.pdf

Gercek, Burcin. 2008. Symantec: Kuinka virustorjunta toimii. Viitattu: 2.3.2013
http://www.symantec.com/region/fi/resources/antivirus.html

Hakala, M. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo

Helle, M. 2004. Etätyö. Helsinki: Edita

Helsingin Yliopisto. 2012. Salasanat. Viitattu 12.10.2012.
http://www.helsinki.fi/helpdesk/ohjeet/kayttoluvat_ja_salasanat/salasanat/hyva_salasana.html

Humak, 2009. Virustorjunta. Viitattu: 2.4.2013.
http://tietohallinto.humak.fi/tietoturva/virustorjunta

Japo, 2009. Ohjeistusta ukkosten varalle. Viitattu: 12.10.2012.
http://www.japo.fi/ohjeet_ukkonen.php

Järvinen, P. 2002. Tietoturva ja yksityisyys. 2. Painos. Jyväskylä: Docendo

Järvinen, P. 2005. Tietokone: Sähköpostin tietoturva. Viitattu 13.10.2012.
http://www.tietokone.fi/lehti/tietokone_2_2005/sahkopostin_tietoturva_2567

Karvonen, T. 2006. Tietoturva kamppaa etätyötä. Viitattu 20.4.2013.
http://www.itviikko.fi/arkisto/2006/06/08/tietoturva-kamppaa-etatyota/20062795/7

Kerttula, E. 2000. Tietoverkkojen tietoturva: Tarpeet ja teknologiat, internet-tietoturva, suljettujen IP-verkkojen tietoturva, julkisen avaimen infrastruktuuri. Helsinki: Edita

Kotilainen, S. 2009. Tietokone: Elisa säästi etätyöllä. Viitattu 12.11.2012.
http://www.tietokone.fi/uutiset/2009/elisa_saasti_2_miljoonaa_etatyolla_ja_verkkokokouksilla

Klemetti, K. 2006. Tietoturvapäivä 2006: Tietoturvasta huolehtiminen on osa liiketoimintaa. Viitattu: 1.3.2013.
http://www.ficom.fi/ajankohtaista/ajankohtaista_1_1.html?Id=1138349941.html

Klensin, J. 2001.RFC 2821: Simple Mail Transfer Protocol. Viitattu: 22.2.2013
ftp://ftp.funet.fi/pub/doc/rfc/rfc2821.txt

Kuivanen, I. 2004. Tietoturva: Varmuuskopiointi. Viitattu 2.2.2013
http://users.metropolia.fi/~kuivi/tietoturva/varmuus.php

Kuivanen, I. 2004. Tietoturva: Tietokoneen suojaaminen. Viitattu 23.3.2013. http://users.metropolia.fi/~kuivi/tietoturva/suojaus.php

Kuivanen, I. 2004. Tietoturva: Käyttäjätunnukset ja salasanat. Viitattu 23.1.2013 http://users.metropolia.fi/~kuivi/tietoturva/salasanat.php

Laaksonen, M. 2006. Yrityksen tietoturvakäsikirja: Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita

Lepistö, K. 2002. Mobiililaite osana monimuoto-opetusta. Viitattu: 3.10.2012. http://people.uta.fi/~as63593/graksa/mobiililaitteita.htm

Microsoft Technet. 2001. Virtual Private Networking: An Overview. Viitattu: 1.5.2013 http://technet.microsoft.com/en-us/library/bb742566.aspx

National Science Foundation, 2008. Telework benefits employers, employees and the environment. Viitattu: 12.11.2012. http://www.nsf.gov/news/news_summ.jsp?cntn_id=111252&org=olpa&from=news

Ojasalo, K. 2009. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. Helsinki: WSOY

OnGuardOnline, 2011. Phishing. Viitattu: 30.10.2012. http://www.onguardonline.gov/articles/0003-phishing

Oulun Yliopisto, 2012. Varmuuskopiointi. Viitattu 4.4.2013 http://www.oulu.fi/tietohallinto/tietoturva/sisalto/tt-kampanja/www_materiaali_1_0/FI/varmuuskopiointi.htm

Panda Software Finland, 2012. Virustorjunta ja cryptography. Viitattu: 20.3.2013 http://www.virustorjunta.net/modules.php?name=Artikkelit&op=viewarticle&artid=3

Pekkola, J. 2002. Etätyö Suomessa: Fyysiset, virtuaaliset, sosiaaliset ja henkiset työtilat etätyöympäristöinä. Helsinki: Svenska Handelshögsola.

Petrasol, 2009. Päivätoimistot ja etätyöpisteet. Viitattu 15.12.2012. http://www.petrasol.fi/palvelukonseptit/business_lounge_-palvelut/paivatoimistot_ja_etatyopisteet/

Repo, K. 2010. Turvattomat salasanat yhä suosittuja. Viitattu: 1.2.2012 http://www.tekniikkatalous.fi/ict/article366581.ece?s=r&wtm=-21012010

RM Education, 2009. Spyware, Adware and Malware - Advice for networks and network users. Viitattu: 10.11.2012. http://www.rm.com/Support/TechnicalArticle.asp?cref=TEC276510

Räty, J. 2005. PC-Tekniikka: Kiintolevyjen tiedon varmistustekniikat. Viitattu 12.12. 2012 http://www.ratol.fi/opensource/pctekniikka/3/kirjat/raid.pdf

Suomen Internetopas, 2010. Tietokonevirukset: Mikä on tietokonevirus? Viitattu: 12.10.2012 http://www.internetopas.com/yleistietoa/virukset/

TAMK, 2008. Tietoturvan osa-alueet. Viitattu: 17.12.2008. http://www.cibernarium.tamk.fi/tietoturva1/osa-alueet_index.htm#tekninen

TE-Palvelut. 2008. Etätyö Viitattu: 20.2.2013 http://www.mol.fi/mol/fi/02_tyosuhteet_ja_lait/0161_etatyo/index.jsp

University of Amsterdam, 2012. Back door. Viitattu: 20.2.2012 http://www.science.uva.nl/~mes/jargon/b/backdoor.html

Symantec, 2008. Suojatun salasanan luominen. Viitattu: 13.10.2012.
http://www.symantec.com/region/fi/corporate/hacker_proof_password.html

Tietoturvaopas, 2012. Perusohjeet: Ajattele enne kuin. Viitattu: 12.5.2012.
http://www.tietoturvaopas.fi/perusohjeet.html

Tietoturvaopas, 2008. Haitoilta suojautuminen. Viitattu: 13.5.2012.
http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haitoiltasuojautuminen.html

Tiedonvälitystekniikka, 1998. Vikasietoisuus ja luotettavuus. Viitattu: 29.10.2012
http://www.netlab.tkk.fi/opetus/s38110/k98/on_line/110l8_14.pdf

VAHTI, 2002. Tietoturvallisuus. Viitattu 4.5.2013.
http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp

Vartiainen, M. 2005. Työministeriö: Mobiilin työn haasteet. Viitattu: 11.10.2012
http://www.mol.fi/mol/fi/99_pdf/fi/06_tyoministerio/06_julkaisut/06_tutkimus/tpt269.pdf

Viestintävirasto, 2013. Tietoturva: Viestinnän salaus. Viitattu 20.4.2013.
https://www.viestintavirasto.fi/tietoturva/palveluidenturvallinenkaytto/viestinnansalaus.html

VPN Consortium, 2008. VPN Technologies: Definitions and Requirements. Viitattu: 5.5.2013.
http://www.vpnc.org/vpn-technologies.html

Vähimaa, A. 2009. Tietokone: Raid-kokoonpanot. Viitattu: 12.12.2012.
http://www.tietokone.fi/lehti/tietokone_3_2009/raid_kokoonpanot_tyopoytakaytossa_418

Webopas, 2012. Tietoturva-Mitkä tiedot kannattaa varmuuskopioida. Viitattu 5.5.2013.
http://www.webopas.net/varmuuskopiointi.html

Ylä-Jääski, V. 2003. MicroPc: Etätyötä turvallisesti. Viitattu: 22.3.2013.
http://mikropc.net/nettilehti/pdf/1004200358.pdf