



TAMPEREEN  
AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

**TIETOTURVAPOLITIIKKA**  
Case: PPCT Finland Oy

**Jarkko Salakari**

Tietojenkäsittelyn koulutusohjelma  
Toukokuu 2007  
Työn ohjaaja: Harri Hakonen

TAMPERE 2007



---

<b>Tekijä(t)</b>	Jarkko Salakari	
<b>Koulutusohjelma(t)</b>	Tietojenkäsittely	
<b>Opinnäytetyön nimi</b>	Tietoturvapoliitikka – Case: PPCT Finland Oy	
<b>Työn valmistumis- kuukausi ja -vuosi</b>	Toukokuu 2007	
<b>Työn ohjaaja</b>	Harri Hakonen	<b>Sivumäärä: 77</b>

---

## TIIVISTELMÄ

Opinnäytetyöni lähtökohdiana on toimeksiantajani PPCT Finland Oy:n tarve tietoturvallisuuden toimintamallien yhdenmukaistamiseksi ylläpitoasiakkaiden kesken. Työn tarkoituksena on luoda yhdenmukainen tietoturvapoliitikka, jota toimeksiantaja voi käyttää tietoturvaratkaisujen toteuttamisen pohjana solmiessaan ylläpitosopimuksia. Työni keskittyy pienille ja keskisuurille yrityksille suunnattuihin ratkaisuihin.

Työn tavoitteena on purkaa tietoturvapoliitikka toimiviksi periaatteiksi ja käytännöiksi, joita toimeksiantaja voi hyödyntää soveltuvilta osin kussakin tapauksessa. Työn pohjana ovat PPCT Finland Oy:ssä yleisesti käytetyt toimintamallit ja ratkaisut yhdistettynä lähdeaineiston tarjoamiin teoreettisiin ratkaisumalleihin. Lisäksi oma kokemus alalta on antanut vahvan pohjan työn toteuttamiselle. Tarkoituksena ei ole tarjota aukottoman yksityiskohtaisia ratkaisuja, vaan pitäytyä yleiskäyttöisissä toimintamalleissa, joita voidaan tapauskohtaisesti soveltaa.

Työ on luonteeltaan tapaustutkimus, joka perustuu vahvasti toimeksiantajalla käytössä oleviin ratkaisuihin. Pääaineistona on käytetty aihetta käsittelevää kirjallisuutta soveltuvilta osin. Kuitenkin lähtökohdaksi on otettu ylläpitoyritys, josta ei suoraan ole tarjolla lähdeaineistoa.

Työn tuloksena on saatu aikaan tietoturvapoliitikka, joka tukee vahvasti toimeksiantajan toimintatapoja. Poliitikka myös määrittelee selkeästi vastuut asiakasyrityksen ja ylläpitäjän välillä, mitä ei aiemmin ole vielä kirjallisesti sovittu. Tietoturvapoliitikkaa on kuitenkin tarkoitus vielä yksilöiviltä osin muokata solmittaessa ylläpitosopimusta asiakkaan kanssa. Pääperiaatteet on tarkoitus pitää samana asiakasorganisaatiosta huolimatta.

Jatkossa nyt kehitellyn politiikan pohjalta on helppo ryhtyä luomaan yrityskohtaista tietoturvasuunnitelmaa, joka määrittelee tietoturvallisuuden toteutustavat kussakin yrityksessä erikseen. Koska pääperiaatteet ovat asiakasyrityksissä samat, ylläpitäjän on helpompi keskittyä työhönsä, tarvitsematta tutustua asiakasyrityksen toimintaan niin yksityiskohtaisesti. Tietoturvapoliitikka tulee varmasti kasvattamaan toimeksiantajan luotettavuutta ja toiminnan laatua asiakasyrityksissä.



---

<b>Author(s)</b>	Jarkko Salakari	
<b>Degree Programme(s)</b>	Business Information Systems	
<b>Title</b>	Information Security Policy – Case: PPCT Finland Oy	
<b>Month and year</b>	May 2007	
<b>Supervisor</b>	Harri Hakonen	<b>Pages: 77</b>

---

## ABSTRACT

The basis of this scholarly thesis is the employer's, PPCT Finland Oy, need for consistent data security practises between clients. The purpose of this job is to develop an information security policy, that can be used as a basis of the data security solutions with new clients. The job is aimed for small and medium sized corporations.

The goal is to give useful principles and practises for data security solutions, that the employer can use in each case. The base of the job are PPCT Finland's common solutions and standards of activity combined in theoretic solutions of the source material. My own experience has created a strong foundation for the job. The purpose is not to give detailed solutions, but to hold on to the general solutions, that can be applied with each customer as needed.

The job is a case study, that is strongly based on the solutions used by the employer. The source material of this scholarly thesis is mainly a literature concerning data security. However no source material is available concerning exclusively companies that provide outsourced information technology maintenance.

The result of this scholarly thesis is an information security policy, that strongly supports the standards of activity used by the employer. The policy also defines the responsibilities between the employer and the client, which has never been written before. The intention is to revise the policy individually when the contract is written with a new client. The main principles are the same in spite of the client.

In the future it is easy for the employer to create individual data security solutions for clients based on this policy. Because the principles are the same with each client, the employees of PPCT don't need so detailed knowledge of each client, so they can concentrate on their work more efficiently. The information security policy will certainly raise PPCT Finland's reliability and quality of service.

# Sisällysluettelo

<b>1 JOHDANTO</b> .....	<b>6</b>
1.1 PPCT FINLAND OY .....	6
1.2 OPINNÄYTETYÖN TAVOITE .....	6
1.3 TIETOTURVALLISUUDEN MÄÄRITELMÄ .....	7
1.4 TIETOTURVAPOLITIikka .....	7
<b>2 HALLINNOllINEN TURVALLISUUS</b> .....	<b>9</b>
2.1 STANDARDEISTA .....	10
2.2 SITOUTUMINEN TIETOTURVAAN .....	12
2.3 LAINSÄÄDÄNNÖN VAATIMUKSET .....	13
2.4 VAKUUTUSYHTIÖIDEN VAATIMUKSET .....	16
2.5 VASTUUT .....	18
2.6 RISKIANALYYSI .....	19
2.7 KOULUTUS JA OHJEISTUS .....	20
2.8 VAITIOLOVELVOLLISUUS .....	21
2.9 HALLINNOllINEN SEURANTA .....	21
<b>3 HENKILÖSTÖTURVALLISUUS</b> .....	<b>23</b>
3.1 PAIKALLINEN TYÖASEMA .....	23
3.2 SISÄVERKKO .....	24
3.3 ETÄKÄYTTÖ JA KANNETTAVAT TIETOKONEET .....	24
3.3.1 VPN (Virtual Private Network) .....	25
3.3.2 WLAN (Wireless Local Area Network) .....	26
3.4 DATAN TALLENTAMINEN .....	26
3.5 TALLENNUSMEDIAT .....	27
3.6 INTERNETIN KÄYTTÖ .....	27
3.7 SÄHKÖPOSTI .....	29
3.7.1 Käyttäjien ohjeistus .....	29
3.7.2 Roskaposti .....	31
3.7.3 Salaustekniikoista .....	34
3.8 KÄYTTÄJÄTILIT .....	36
3.9 SALASANAT .....	37
<b>4 FYYSINEN TURVALLISUUS</b> .....	<b>38</b>
4.1 KULUNVALVONTA .....	38
4.2 MURTOVAHINKOJEN TORJUNTA .....	39
4.3 SÄHKÖVAHINKOIHIN VARAUTUMINEN .....	40
4.4 PALO- JA VESIVAHINKOIHIN VARAUTUMINEN .....	41
4.5 VARMUUSKOPIOT, ASENNUSMEDIAT JA LISENSSIT .....	42
4.6 LAITTEISTOTURVALLISUUS .....	43
4.6.1 Laitteistojen fyysinen lukitus .....	43
4.6.2 Turvamerkinnät .....	44
4.6.3 Laitteistojen ja komponenttien oikeaoppinen hävittäminen .....	45

<b>5 TIETOLIIKENNETURVALLISUUS .....</b>	<b>47</b>
5.1 UHKATEKIJÄT TIETOVERKOISSA .....	47
5.2 DOKUMENTOINTI .....	49
5.3 JÄRJESTELMÄN- JA KÄYTÖNVALVONTA .....	50
5.4 REITITYS JA KYTKIMET .....	52
5.5 PALVELIMET .....	52
5.6 PALOMUURIT .....	54
5.7 VIRUSTORJUNTA .....	58
5.8 OHJELMISTOTURVALLISUUS .....	59
5.9 TIETOAINESTOTURVALLISUUS .....	60
5.9.1 Tiedon luokittelu .....	61
5.9.2 Varmuuskopiointi .....	63
<b>6 TIETOTURVAPOLITIIKAN TOTEUTUS .....</b>	<b>68</b>
<b>7 YHTEENVETO .....</b>	<b>70</b>
<b>LÄHTEET .....</b>	<b>71</b>
<b>LIITTEET .....</b>	<b>74</b>
LIITE 1: PPCT FINLAND OY – TIETOTURVAPOLITIIKKA .....	74

# 1 Johdanto

## 1.1 PPCT Finland Oy

Opinnäytetyön toimeksiantaja PPCT Finland Oy on Tampereen Vehmaisissa toimiva IT-, ohjelmisto- ja markkinointipalveluita tuottava yritys. PPCT:n palveluksessa on 21 työntekijää, joista 6 toimii osittain tai kokonaan IT-palveluiden parissa. Yrityksen liikevaihto on noin 1,5 miljoonaa euroa (helmikuu 2007).

PPCT Finland Oy on nykymuodossaan perustettu keväällä 2005 ja se on muotoutunut vuonna 1994 perustetusta Pirkanmaan PC-tuotteet Oy:stä. Yrityksen toimitusjohtaja ja perustaja on Aarre Siljanpää.

PPCT on kevääseen 2007 mennessä palvellut noin 1100 asiakasta. Aktiivisia ylläpitoasiakkaita, eli jatkuvaa ylläpitoa vaativia asiakkaita yrityksellä on noin 20, joista suurin osa toimii pääasiassa Pirkanmaan alueella.

Itse suoritin PPCT Finland Oy:ssä Tampereen ammattikorkeakoulun työharjoittelujakson heinä-marraskuussa 2006. Työtehtäväni käsittivät pääasiassa asiakkaiden työasema- ja palvelinasennuksia, huoltotoimintaa sekä mikrotukitehtäviä. Varsinaisen kipinän tälle opinnäytetyölle antoi kuitenkin viikoittainen asiakkaan palvelin-toiminnan seuranta sekä erilaiset asiakaskäynnit. Nämä tehtävät käynnistivät ajatusprosessin tietoturvallisuuteen vaikuttavista osatekijöistä, joka lopulta johti opinnäytetyön kirjoittamiseen aiheesta.

## 1.2 Opinnäytetyön tavoite

Opinnäytetyön tavoitteena on luoda tietoturvapoliittikka PPCT Finland Oy:lle, jota voidaan käyttää pohjana ylläpitoasiakkaiden tietoturvallisuusasioiden hoidossa.

Päämääränä on siis luoda yleispätevä ratkaisu, jota voidaan täydentää yksilöiviltä osin solmittaessa ylläpitosopimusta asiakkaan kanssa. Tietoturvallisuusasioiden hoito pyritään tietoturvapoliittikan avulla yhdenmukaistamaan niin, että samat periaatteet ohjaavat toimintaa asiakasorganisaatiosta riippumatta.

Opinnäytetyössä pyritään ottamaan mahdollisimman laajasti huomioon kaikki tietoturvallisuuteen vaikuttavat osatekijät ja etsimään niille ratkaisumallit.

Tietoturvallisuus jaetaan työssä osa-alueisiin, joiden kautta tietoturvapoliittikkaa lähdetään purkamaan yksittäisiin toimenpiteisiin

ja käytäntöihin, joita tietoturvallisuuden kokonaisvaltainen toteutuminen edellyttää.

### **1.3 Tietoturvallisuuden määritelmä**

Tietoturvallisuudella tarkoitetaan tietojenkäsittelyn turvaamista. Sen avulla pyritään toteuttamaan seuraavat periaatteet:

*Käytettävyys* tarkoittaa että tiedot ovat saatavissa oikeassa muodossa ja riittävän nopeasti.

*Eheys* tarkoittaa että tietojärjestelmän tiedot ovat luotettavia, eli ne eivät sisällä tahallisia tai tahattomia virheitä.

*Luottamuksellisuus* tarkoittaa että tiedot ovat vain oikeutettujen henkilöiden käytettävissä.

*Kiistämättömyys* merkitsee järjestelmän kykyä tunnistaa ja tallentaa luotettavasti käyttäjän tiedot. Kiistämättömyydellä tahdotaan varmistaa tiedon alkuperä ja tunnistaa niiden luvaton käyttö.

*Pääsynvalvonta* tarkoittaa niitä menetelmiä, joilla rajoitetaan tietojärjestelmän käyttöä. (Hakala & Vainio & Vuorinen 2006: 4 - 6)

Näiden lisäksi on olemassa kuudes periaate, josta käytetään nimeä todennus tai autenttisuus. *Todennus* tarkoittaa eri osapuolten luotettavaa tunnistusta. Todennus on kuitenkin luottamuksellisuuden ja kiistämättömyyden perusedellytys, joten se jätetään usein pois tietoturvallisuuden määritelmästä. (Järvinen 2003: 29 - 34)

### **1.4 Tietoturvapoliittikka**

Tietoturvapoliittikka on organisaation, tässä tapauksessa toimeksiantajan ja asiakasorganisaation johdon hyväksymistä tietoturvalisuuskäytännöistä ja –periaatteista koostuva dokumentti. Tietoturvapoliittikan on tarkoitus olla voimassa keskipitkän tai pitkän (n. 5-10 vuotta) aikavälin ohjeena kaikille tietojärjestelmän käyttäjille. Näin ollen siihen ei sisällytetä yksityiskohtaisia ratkaisuja, jotka muuttuessaan vaatisivat tietoturvapoliittikan päivittämistä. Poliittikka tulee kuitenkin tarkastaa vuosittain, jotta varmistutaan sen pätevyydestä mahdollisten muutosten jälkeenkin. Poliittikka on julkinen, joten se ei saa sisältää tietoja joita hyökkääjä voisi käyttää hyväkseen päästäkseen käsiksi organisaation tietojärjestelmään. Kuitenkaan se ei saa olla liian yleisluontoinen, sillä se on tärkein organisaation tietoturvallisuutta ohjaava dokumentti. (Hakala ym. 2006: 7 - 8)

Hyvä tietoturvapoliittikka sisältää organisaatioiden tietoturvallisuuden määritelmän, keskeiset kohteet ja laajuuden. Se esittää turvallisuuden tärkeyden organisaation toiminnalle ja sen jatkuvuudelle sekä rakenteet joilla tietoturvallisuuteen pyritään. Se sisältää myös yhteenvedon tietoturvakäytännöistä ja periaatteista sekä lainsäädännön ja sopimusten tietoturvallisuudelle asettamista vaatimuksista. Siinä esitellään myös yhteenveto turvallisuusajattelun edistämistoimista ja turvallisuuskoulutuksen järjestämisestä. Tietoturvapoliittikassa määritellään tietoturvallisuuteen liittyvät vastuualueet ja ohjeet turvallisuuteen vaikuttavien tapahtumien raportoinnista. Lisäksi politiikka sisältää seuraukset tietoturvallisuuspolitiikan rikkomuksista sekä luettelon politiikkaa tarkentavista dokumenteista. (Hakala ym. 2006: 8 - 9)

Tietoturvapoliittikka kirjoitetaan niin, että sen voi ymmärtää kuka tahansa lukija. Tietoturvapoliittikan liitteet kuvaavat tarkemmin käytännöt ja tekniset ratkaisut, joten ne ovat luonteeltaan salaisia tai luottamuksellisia. (Hakala ym. 2006: 9)

Tärkein tietoturvapoliittikan tehtävä on, että sen avulla yrityksen johto voi määritellä miten turvallisuusasioihin suhtaudutaan. Tietoturvapoliittikka on organisaation johdon kannanotto, joten se on luonteeltaan lyhyt ja ytimekäs. (Miettinen 1999: 145)

Koska asiakasorganisaatio on tässä tapauksessa ulkoistanut tietojärjestelmiensä ylläpidon, sen on pystyttävä varmistumaan tietojensa salassapidosta ja tietoturvallisuuden noudattamisesta. Samaan tapaan ylläpitäjän on varmistuttava siitä, että myös asiakasorganisaatio ottaa toiminnassaan huomioon tietoturvallisuuden. Tämän varmistamiseksi voidaan käyttää erillistä salassapitosopimusta, joka solmitaan ylläpitäjän ja asiakasorganisaation kesken. (Miettinen 1999: 140 - 143)

Tässä tapauksessa kuitenkin järkevämpi ratkaisu on sitoa salassapitosopimus tietoturvapoliittikkaan, jolloin osapuolten välillä ei tarvitse käyttää useita erilaisia dokumentteja. Näin ollen ylläpitosopimus- ja tietoturvapoliittikkadokumentit yhdessä muodostavat ylläpitosopimukselle luotettavan pohjan.

Koska toimeksiantaja pyrkii mahdollisuuksien mukaan yhtenäistämään asiakasorganisaatioiden tietoturvallisuusasioiden hoidon, se helpottaa huomattavasti asiakkaiden tietojärjestelmien ylläpitoa. Näin ylläpitäjä tietää tarkalleen vastuunsa ja sen vaatimat toimenpiteet asiakkaasta riippumatta. Lisäksi tietoturvapoliittikka varmasti kasvattaa toimeksiantajan palvelun laatua ja antaa sidosryhmille luotettavan ja vakuuttavan kuvan organisaatiosta.



## 2 Hallinnollinen turvallisuus

Pohjois-Karjalan ammattikorkeakoulun teettämän tutkimuksen mukaan henkilöstöturvallisuus ja hallinnollinen turvallisuus ovat alkuvuodesta 2005 olleet yritysten tietoturvan heikoimpia osaluokkia. 44% tutkituista 32:sta Pohjois-Karjalassa vaikuttavasta yrityksestä ei järjestä lainkaan tietoturvakoulutusta uusille työntekijöille. Lisäksi riskien kartoittaminen ja tietoturvapoliittikka ovat olleet yrityksissä heikosti toteutettuja. Sen sijaan tekninen tietoturva on toteutettu hyvin. Kyseinen artikkeli kertoo kiistatta että tietoturva mielletään lähinnä tekniseksi ongelmaksi jolloin unohdetaan kaksi perustavanlaatuista tekijää, eli hallinnollinen turvallisuus ja henkilöstöturvallisuus. Kokonaisvaltaisen turvallisuuden ylläpitämisen sijaan siis torjutaan tietoturvaloukkauksia. (Karjalainen, 22.3.2005.) Mainittu ajattelutapa on rinnastettavissa väistämättä länsimaisen lääketieteen perusongelmaan, jossa terveyden sijaan hoidetaan oireita.

Hallinnollinen turvallisuus kokoaa kaikki tietoturvallisuuden osaluokkia yhtenäiseksi kokonaisuudeksi. Hallinnollisen turvallisuuden tehtävä on käytännössä luoda edellytykset tietoturvallisuuden ylläpidolle ja kehittämiselle. (Miettinen 1999: 18)

Hallinnollinen turvallisuus käsittelee tietoturvan kehittämiseen ja johtamiseen liittyviä asioita. Erityisen tärkeää on lainsäädännön ja erilaisten sopimusten, kuten vakuutus sopimusten vaikutusten arviointi tietoturvakäytäntöihin. (Hakala ym. 2006: 10 - 11)

Hallinnollisen turvallisuuden lähtökohtana on organisaation johto ja sen sitoutuminen tietoturvaluokkaan. Erityisen tärkeitä asioita ovat myös vastuun jakaminen, sekä henkilöstön koulutus ja ohjeistus. (Rousku 2003: 54 – 56.) Lisäksi tässä luvussa käsitellään myös vaihtoehtoisuus, joka on eräänlainen keino henkilöstön sitoutumisen edistämiseksi.

Edellisten lisäksi tässä luvussa käydään läpi keskeiset kohdat tietoturvaluokkaan liittyvistä standardeista. Standardit ovat tietoturvaluokkaan kehittämisen kannalta hyvä lähtökohta, joskaan tässä tapauksessa ei suoraan lähdetä luomaan suoranaisesti standardien mukaista tietoturvaratkaisua.

Riskianalyysi on niin ikään hyvä lähtökohta tietoturvasuunnittelulle, joten sen suorittamiseen tutustutaan myös. Viimeisenä alakohdassa käsitellään hallinnollinen seuranta, joka tarkoittaa asiakasorganisaation suorittamaa seuranta organisaatiossa. Se on erotettu omaksi alakohdaksi sen vuoksi, ettei asiakasorganisaatio saa unohtaa omaa vastuutaan tietoturvaluokkaan noudattamisen seu-

rannassa. Ylläpitäjän toimesta tässä tapauksessa voidaan keskittyä lähinnä tekniseen seurantaan, jota käsitellään myöhemmin.

## 2.1 Standardeista

Kansainvälisiä standardeja on luotu tietoturvasuunnittelua varten. Niistä käytetään nimitystä ”tietoturvastandardi”, vaikka ne eivät anna varsinaisia vaatimuksia itse tietoturvalle, vaan sen suunnitteluun. On syytä kuitenkin muistaa, että standardien noudattaminen ei sinällään takaa riittävää turvallisuutta. (Hakala ym. 2006: 46.) Opinnäytetyössä käsitellään tarkemmin ISO/IEC 17799 –standardi (ISO = International Organization of Standardization), joka on yleisluontoinen ja soveltuu näin erilaisille yrityksille ja yhteisöille. Koska alkuperäistä englanninkielistä standardia ei tämän opinnäytetyöprojektin aikana ole löytynyt lainakokoelmista ja sen ostaminen ei tule kyseeseen, käytetään tältä osin lähdemateriaalina Tietoturvallisuuden käsikirjan tiivistettyä suomenkielistä kuvausta kyseisestä standardista.

ISO/IEC 17799 –standardi sisältää yleiset periaatteet tietoturvallisuuden suunnitteluun, ylläpitoon ja kehittämiseen. Standardi on jaettu yhteentoista klausuuliin, eli lukuun (security control clause), joissa kussakin 1-10 pääkategoriaa (main security category). Jokaiseen kategoriaan liittyy tavoitemäärittely (control objective) ja ohjaustoimintoja (control) joilla tavoitteisiin päästään. Kuvauksia on selvitetty toteutusohjeilla (implementation guidance), sekä lisätiedoilla (other information). Standardi ei ole sinällään sitova, mutta se on ”keskeisin tietoturvasuunnittelun sisältöä ohjaava standardi”. (Hakala ym. 2006: 46 - 47)

Seuraavassa esitetään ISO/IEC 17799 –standardin pääkohdat, kuten Tietoturvallisuuden käsikirjassa (Hakala ym. 2006: 47 - 48) on määritelty:

1. Riskianalyysi, riskien evaluointi ja käsittely (Risk assessment and treatment). Kohta käsittelee systemaattista riskien hakua, riskeihin suhtautumista ja niiden vaikutusten arvioimista.
2. Turvallisuuspolitiikka (Security policy). Tietoturvapolitiikan määrittely, sisältö, sekä levittäminen organisaatiossa ja sen sidosryhmissä, painottaen johdon sitoutumista tietoturvan toteuttamiseen.
3. Tietoturvallisuuden organisointi (Organization of information security). Käsitellään tietoturvan sisällyttämistä kaikkeen organisaation toimintaan ja toimintaan sidosryhmien kanssa. Lisäksi käsitellään toiminnan koordinoimista, säännöllistä tarkastelua sekä vastuun jakamista.

4. Omaisuuden hallinta (Asset management). Asset-termi määritellään tarkoittamaan kaikkia aineellisia ja aineettomia hyödykkeitä, joilla on organisaation toiminnan kannalta merkitystä. Kohdassa käsitellään omaisuuden sallitun ja kielletyn käytön määrittelyä, inventointia, omistajuuden määrittelyä sekä tietojen luokittelujärjestelmän luontia.

5. Henkilöstöturvallisuus (Human resources security). Käsitellään henkilöstön ja yhteistyökumppaneiden roolit ja vastuut, sopimukset, taustaselvitykset, johdon vastuu, kurinpitotoimet ja työsuhteen päättymisen.

6. Fyysinen ja ympäristöturvallisuus (Physical and environmental security). Käsitellään tietojenkäsittelyn määrittely ja suojaaminen, kulun- ja käytönvalvonta, laitteiston ja kaapeloinnin suojaaminen, työskentely organisaation ulkopuolella sekä laitteistojen kierrätys ja hävittäminen.

7. Käytön hallinta (Communications and operations management). Dokumentoidut toimintatavat ja vastuut, muutosten hallinta, tehtävien eriyttäminen, kehityksen, testauksen ja tuotannon eriyttäminen, ulkoisten palveluiden hallinta, järjestelmien suunnittelu ja hyväksyttäminen, haittaohjelmilta suojautuminen, tietojen varmistus, tietoliikenneturvallisuuden hallinta, tietovälineiden käsittely, järjestelmädokumenttien turvallisuus, tiedon välitys organisaation ja sen sidosryhmien välillä, sähköinen kauppa sekä käytön valvonnan menetelmät.

8. Pääsyn valvonta (Access control). Pääsynvalvontapolitiikka, pääsynvalvonnan hallinta, käyttäjien vastuut, verkon pääsynvalvonta, käyttöjärjestelmien ja varusohjelmien käytön rajoittaminen, sovellusten ja tietojen käytön rajoittaminen sekä mobiilikäyttöä koskevat rajoitukset.

9. Tietojärjestelmien hankinta, kehittäminen ja ylläpito (Information systems acquisition, development and maintenance). Turvallisuusvaatimusten analysointi ja määrittely, eheyden varmistaminen sovelluksissa, salaustekniikoiden käyttö, järjestelmätiedostojen turvallisuus, sovelluskehityksen ja tukiprosessien turvallisuus sekä tekninen haavoittuvuuksien hallinta.

10. Tietoturvatapahtumien hallinta (Information security incident management). Tietoturvatapahtumien ja heikkouksien raportointi sekä ei-toivottujen tapahtumien hallinta ja turvallisuuden parantaminen.

11. Toiminnan jatkuvuuden hallinta (Business continuity management). Tietoturvallisuuden sulauttaminen osaksi organisaation yleistä jatkuvuuden hallintaa.

12. Yhteensopivuus (Compliance). Yhteensopivuus lainsäädännön ja sopimusten kanssa, standardien mukaisuus, vastaavuus organisaatiossa noudatettaviin käytäntöihin, tekninen yhteensopivuus sekä auditointi.

Toinen yleisluontoinen standardi on ISO/IEC 27001 –standardi, joka on merkittävästi sitovampi kuin ISO/IEC 17799 –standardi. Mikäli yritys tahtoo auditoida ja sertifioida tietoturvallisuuden hallintajärjestelmänsä, tulee sen sisältää standardin klausuulit 4-8. Standardia ei voi seurata ilman ISO/IEC 17799 –standardia. Standardin perusajatuksena on tietoturvallisuuden hallintajärjestelmän prosessinomainen kehittäminen PDCA-mallin (Plan, Do, Check, Act) mukaisesti. (Hakala ym. 2006: 49 – 50.) Tätä standardia ei kuitenkaan käsitellä opinnäytetyössä, sillä kyseinen standardi on luonteeltaan sitova. Tässä yhteydessä ei tahdota suoranaisesti sitoutua standardeihin, vaan lähinnä käyttää niitä hyväksi tietoturvasuunnittelussa.

## *2.2 Sitoutuminen tietoturvaan*

Kuten vanha sanontakin kertoo, joukko on johtajansa näköinen. Kaikki lähtee siitä, kuinka yrityksen johto on sitoutunut tietoturvan noudattamiseen. Mikäli sitoutuminen ei ole aitoa ja jatkuvaa, ei tietoturvallisuusasioiden tehokas hoitokaan ole mahdollista. Johdon sitoutumisella tietoturvallisuus saadaan sisällytettyä osaksi yrityksen päivittäisiä liiketoimintaprosesseja. Niinpä tietoturvallisuus tulee nähdä liiketoimintaa vahvasti tukevana tekijänä. Tilanetta ei saa päästää siihen pisteeseen, että organisaatio joutuu kohtaamaan jonkun merkittävän tietoturvaloukkauksen ja sen kautta vasta alkaa arvioida tietoturvallisuuden merkitystä. Näin valitettavan usein kuitenkin toimitaan. (Miettinen 1999: 44, 48)

Tietoturvallisuus muodostuu osaksi liiketoimintaa asteittain. Kaikki lähtee siitä, että johdon on tiedostettava tietoturvallisuuden merkitys. Kun sen merkitys on tiedostettu, johto sitoutuu tietoturvallisuuden ylläpitoon ja kehittämiseen ja näin tietoturvallisuus muovautuu osaksi organisaation toimintaprosesseja ja yrityskulttuuria. Lopulta tietoturvallisuuden pitkäjänteinen kehittäminen ja kokonaisvaltainen noudattaminen tekevät siitä yrityksen kilpailutekijän. Se voi näkyä hyvänä asiakaspalveluna, laadukkaina tuotteina ja julkisuudessa luottamusta herättävänä yrityskuvana. Lopulta pystytään huomaamaan kuinka tietoturvallisuus voi vaikuttaa liiketoimintaa kasvattavasti. Näin ollen tietoturvallisuutta voidaan pitää eräänlaisena oravanpyöränä. Kun panostetaan tietoturvaluuteen,

panos tulee lopulta moninkertaisena takaisin kehityskierroksen jälkeen. (Miettinen 1999: 46 - 48)

Se että tässä tapauksessa yritys on ulkoistanut IT-toimintonsa ei muuta sitoutumisen tarvetta. Kun käytetään ulkoistettua palvelua IT-asiantuntijat eivät voi joka hetki valvoa juuri kyseisen yrityksen toimintoja. Tällöin suuri osa vastuusta siirtyy asiakasyrityksen kontolle. Ylläpitäjän vastuulle siirtyy tietenkin tietoturvaan liittyvien teknisten ratkaisujen toteuttaminen, mutta vastuu tietoturvallisesta toiminnasta säilyy pääosin asiakasyrityksellä.

Yrityksen johdon tehtävä on huolehtia siitä, että jokainen työntekijä osaltaan sitoutuu noudattamaan tietoturvasäännöstöä. Tämä merkitsee tarvittavan koulutuksen ja ohjeistuksen järjestämistä tietoturva-asioihin liittyen. Unohtaa ei saa kuitenkaan sitä, että yrityksen johto toimii esimerkkinä henkilöstölleen. Näin ollen henkilöstön tietoturvallisen toiminnan takaaminen vaatii yrityksen johdon vahvaa ja jatkuvaa sitoutumista tietoturvallisuuden toteuttamiseen. Haasteellista on henkilöstön motivoiminen tietoturvan noudattamiseen. Vanhasta kokemuksesta kiellot ja määräykset eivät aina ole paras keino tietoturva-asioiden hoitamiseen, ne saattavat tarkoituksen vastaisesti aiheuttaa jopa negatiivisia miellelyhtymiä tietoturvasta, jolloin rikkomusten riski luonnollisesti kasvaa. Ehkä paras keino saattaakin olla tietoturva-asioiden yhteyttäminen päivittäisiin rutiineihin ja vaadittujen toimenpiteiden perusteleminen työntekijälle. (Hakala ym. 2006: 114)

ISO/IEC 17799 –standardin toisessa pääkohdassa korostetaan johdon sitoutumista ja tiedon levittämistä organisaation sisällä sekä sen sidosryhmien välillä. (Hakala ym. 2006: 47)

Kyseinen standardi määrittelee keinot joilla yrityksen johto osoittaa sitoutumisensa tietoturvaan. Tässä tapauksessa huomioon otettavia keinoja ovat mm. tietoturvallisuuden edellyttämien roolien ja vastuiden määrittely. Tietoturvallisuuden tavoitteiden, tietoturva-politiikan mukaisen toiminnan tärkeyden sekä organisaation juridisen vastuun selkeä ilmaiseminen henkilöstölle. Lisäksi turvallisuusasioiden säännöllisten tarkastusten järjestäminen. Organisaation johdon tulee ehdottomasti miettiä näitä asioita, sillä pelkkä tietoturvapoliittikadokumentti ei riitä osoitukseksi tietoturvallisuuden sitoutumisesta. Luonnollisesti se ei myöskään riitä henkilöstön motivoimiseksi tietoturvalliseen toimintaan. (Hakala ym. 2006: 114)

### ***2.3 Lainsäädännön vaatimukset***

ITViikko-lehdessä vuonna 2004 julkaistussa Ernst & Youngin tietoturvaselvityksessä haastateltiin 1233 yritystä 51:stä maasta. Sen

mukaan 80 % yrityksistä ei tarkista ylläpitopalvelun tuottajan tietoturvapoliittikan ja lain yhteensopivuutta. Lisäksi 70 % yrityksistä ei tarkasta oman ja ylläpitäjän tietoturvapoliittikan yhteensopivuutta. (Ernst & Young: Tietoturvariskejä... 2004)

Lainsäädäntö tulee kuitenkin aina ottaa huomioon soveltuvilta osin. Koska Suomessa ei ole yhtenäistä tietoturvallisuuslainsäädäntöä, tietoturvallisuutta koskevia säännöksiä sisältyy useisiin eri lakeihin ja asetuksiin. Sama pätee henkilötietojen käsittelyyn ja luottamuksellisen viestinnän turvaamiseen. (Sähköisen viestinnän... 2006.) Tämän vuoksi myöskään kaikkien tietoturvallisuutta koskevien lainkohtien yksityiskohtainen käsittely tässä opinnäytetyössä ei ole käytännössä mahdollista. Tässä luvussa pyritään lähinnä osoittamaan tietoturvallisuuden suunnittelussa ja toteutuksessa sovellettavat olennaisimmat lainkohdat, jotka tietoturvaratkaisuja suunniteltaessa on olennaista ottaa huomioon.

Sähköisen viestinnän tietosuojalain ”tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä.” Lakia sovelletaan pääasiassa yleisissä viestintäverkoissa tarjottaviin tele- ja verkkopalveluihin. Kuitenkin lain 4§ ja 5§ pykälä koskee myös sisäisiä verkkoja, eli tässä tapauksessa asiakasorganisaation verkkoa. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516)

Neljännän pykälän perusteella viesti, tunnistamis- ja paikkatiedot ovat luottamuksellisia, elleivät ne ole saatettu julkisesti vastaanotettaviksi. Viestiin liittyvät tunnistamistiedot ovat joka tapauksessa luottamuksellisia. Viidennessä pykälässä puolestaan käsitellään vaitiolovelvollisuutta ja hyväksikäyttökieltoa. Käytännössä se, joka on vastaanottanut tai saanut tiedon toiselle ihmiselle osoitetusta luottamuksellisesta viestistä tai sen tunnistamistiedoista, ei saa ilman lähettäjän tai vastaanottajan lupaa ilmaista tai käyttää tietoa hyväksi. Sama pätee paikkatietoihin, joita ei saa ilman paikannettavan lupaa paljastaa tai käyttää hyväksi. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516)

Henkilötietolain ”tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.” Käytännössä laki vaatii organisaatiota määrittelemään miksi tietoja kerätään ja kuinka niitä käsitellään, sekä käytettävät tietolähteet ja säännöt tietojen luovutukseen. Periaatteena on, että kerättyjä tietoja saa käyttää vain siihen tarkoitukseen, johon ne on kerätty. Luonnollisesti laki velvoittaa organisaatiota kaikessa toiminnassa, joten se on otettava huomioon myös

tietoturvallisuuden kannalta. Oikeudellisten seuraamusten uhalla on huolehdittava arkaluontoisten tietojen käsittelystä organisaatiossa ja siitä, etteivät ne pääse leviämään organisaation ulkopuolelle oikeudetta. (Henkilötietolaki 22.4.1999/523)

Laki yksityisyyden suojasta työelämässä on erittäin olennainen organisaation kaikessa toiminnassa. ”Lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä.” (Laki yksityisyyden suojasta työelämässä 13.8.2004/759)

Tietoturvallisuuden kannalta tulee erityisesti ottaa huomioon lain pykälät 16§ ja 17§, joissa määritellään kameravalvonnan säännöt. Käytännössä laki edellyttää, ettei tiettyjä työntekijöitä saa valvoa, ellei valvontaa toteuteta vaaran tai rikosten ehkäisemiseksi tai työntekijän etujen varmistamiseksi. Lisäksi on huomioitava pykälät 18§, 19§ ja 20§, joissa käsitellään määräyksiä työnantajalle kuuluvien sähköisten viestien esille hakemista ja avaamista. Pykälien keskeinen sisältö on, ettei työnantaja saa hakea esille työntekijän sähköpostiviestejä ilman työntekijän lupaa. Poikkeustilanteet ja viestien hakua koskevat menettelytavat tuodaan myös esille laissa. Pykälä 21§ määrittelee ilmoitusvelvollisuudesta työntekijöille, mikäli heitä valvotaan jollain teknisellä menetelmällä. Lisäksi on määriteltävä valvonnan käyttötarkoitus ja käytettävät menetelmät. (Laki yksityisyyden suojasta työelämässä 13.8.2004/759)

Edellisten lisäksi tietojen arkistointiin liittyvät määräykset tuo ilmi Arkistolaki, jota on syytä seurata soveltuvin osin. (Arkistolaki 23.9.1994/831)

Viestintävirastolla on myös kattava kokoelma määräyksiä, jotka koskevat kuitenkin lähinnä teleoperaattoreita ja tietoverkkopalveluiden tarjoajia. Määräyksiä ei siis sovelleta yksityisiin verkkoihin. Kuitenkin tietoturva suunniteltaessa, niistä saa tärkeää tietoa tietoturvallisuudessa huomioon otettavista seikoista, joten niihin kannattaa tutustua kattavan tietoturvaratkaisun aikaansaamiseksi. Tässä opinnäytetyössä otetaan esille kaksi tietoturvaratkaisujen suunnittelun kannalta hyödyllistä Viestintäviraston määräystä, joita voidaan käyttää tässä yhteydessä lähinnä kattavina ohjedokumentteina.

Määräys teleyritysten tietoturvasta määrittelee yksityiskohtaisesti tietoturvallisuuden osa-alueet ja mitä ne käytännössä vaativat organisaatiolta. (Viestintävirasto 47 B/2004 M)

Määräys viestintäverkon fyysisestä suojaamisesta käsittelee tietojärjestelmätilojen fyysistä suojaamista erittäin perusteellisesti. Tä-

mä onkin viisasta lukea, mikäli organisaation fyysistä tietoturvaa halutaan parantaa. (Viestintävirasto 48 B/2004 M)

## **2.4 Vakuutusyhtiöiden vaatimukset**

Vakuutusyhtiöiden tietoturvallisuusvaatimukset puolestaan vaihtelevat eri vakuutusyhtiöiden välillä, joten tässä opinnäytetyössä käytetään siltä osin lähteenä Suomen Vakuutusyhtiöiden Keskusliiton suojeleohjetta. Suojeleohje ei ole sinällään vakuutusyhtiötä sitova, vaan jokainen vakuutusyhtiö saa käyttää suojeleohjetta haluamillaan osin vapaasti omissa vakuutusehdoissaan. Tämän vuoksi tietoturvallisuusratkaisun suunnittelussa tulee ensisijaisesti ottaa huomioon sen vakuutusyhtiön vakuutusehdot, josta laitteiden vakuutukset aiotaan hankkia. (Tietotekniikkalaitteiden... 2003)

Suomen Vakuutusyhtiöiden Keskusliiton Tietotekniikkalaitteiden katoamisten ja varkauksien ehkäisy –suojeleohjeessa puututaan mm. seuraaviin tietoturvallisuusasioihin:

Kannettaviin tietokoneisiin suositellaan vaijerikiinnitysmahdollisuutta, jolla kannettava laite voidaan lukita kiinteään kalustukseen myös matkoilla ja ajoneuvoissa säilytettäessä. Kiinteästi asennettujenkin laitteiden fyysistä lukitusta suositellaan varsinkin julkisissa tiloissa.

Tiedon varmistukset suositellaan otettavaksi suoraan palvelimille, ei erillisille tietovälineille. Uudelleenkirjautumista vaativaa näytönsäästäjää suositellaan. Eli mikäli tietokoneen näytönsäästäjä on aktivoitunut, koneeseen ei pääse käsiksi ilman käyttäjätunnusta ja salasanaa.

Salassa pidettävän tiedon tallennusta kannettavan tietokoneen kiintolevyille on vältettävä, tarvittaessa käytettävä salakirjoitusta. Arvokasta ja luottamuksellista tietoa sisältävä kiintolevy tulee voida irrottaa kannettavasta tietokoneesta, niin ettei sitä säilytetä samassa tilassa tietokoneen kanssa.

Käyttäjätunnusta ja säännöllisesti muutettavaa salasanaa vaaditaan. Vaihtoehtoisia tunnistusmenetelmiä ovat toimikortti ja biometrinen tunnistus.

Toimikortti on luottokortin kokoinen muovikortti, eli ns. älykortti. Siihen upotettu siru sisältää varmenteen jolla käyttäjä tunnistetaan. Lisäksi se huolehtii tarvittavien matemaattisten operaatioiden suorittamisesta. Periaatteessa toimikortti on tavallaan pieni tietokone, ilman näppäimistöä ja näyttöä. (Järvinen 2003: 173 - 176)



Biometrinen tunnistus tarkoittaa ihmisen ominaisuuksiin perustuvaa tunnistusta. Käytännössä äänen tunnistus ja sormenjälkitunnistus on nykyaikana mahdollista. (Järvinen 2003: 36) Yleisimmin biometrisistä menetelmistä käytetään sormenjälkeen perustuvaa tunnistusta. Esimerkiksi IBM:n nykyaikaisissa kannettavissa tietokoneissa on yleisesti sormenjälkitunnistumahdollisuus.

Pysäköityä ajoneuvoa, jossa tietokonetta säilytetään on pidettävä silmällä ja vältettävä pysäköintipaikkoja jossa se joutuu alttiiksi murtovarkauksille. Yöpymisen ajaksi tietokonetta ei saa jättää ajoneuvoon, mutta poikkeustilanteessa se on lukittava kiinni ajoneuvoon. Konetta ei pidä ajoneuvon avaamisen tai lukitsemisen ajaksi sijoittaa paikkaan johon se voi unohtua.

Julkisissa kulkuneuvoissa tietokone on kuljetettava käsimatkatavarana jatkuvan valvonnan alla. Kannettavan tietokoneen kantolaukusta ei saisi pystyä päästelemään sen sisältöä. Turhaa kuljettamista tulee aina välttää.

Kiinteästi asennettujen tietokoneiden suojaamiseksi kiinteistön ulko-ovet on pidettävä lukittuina ja ikkunat kiinni työajan ulkopuolella. Avaimet on säilytettävä lukitussa paikassa, josta vain valtuutettu vastuhenkilö saa niitä luovuttaa. Riskialttiissa ympäristössä kuten katutasossa suositellaan murronkestäviä ikkunoita. Katutasossa sijaitseva liikehuoneisto tulee lisäksi valaista ulkopuolelta pimeään aikaan.

Murtovarkauksien ehkäisemiseksi suositellaan rikosilmoituslaitteistoa, joka antaa sekä paikallisen, että vartiointiliikkeelle suunnatun hälytyksen. Rikosilmoituslaitteistolla valvotaan kiinteistön ovia, ikkunoita ja sisätiloja. Varashälytintä suositellaan myös matkoilla ja ajoneuvoissa. Tallentavaa videovalvontajärjestelmää niin ikään suositellaan. Ulkopuolisten pääsyä tiloihin ja liikkumista tulee valvoa kulunvalvonnalla ja vastaanottojärjestelyin.

Laitteista tulee pitää ajantasaista laiteluetteloa, jonka tulee perustua turvamerkintöihin tai sarjanumeroihin. Turvamerkintää suositellaan erityisesti kannettaviin laitteisiin ja sen olemassaolosta ilmoittava tarra on liimattava laitteeseen.

Kotona olevat laitteet eivät saa näkyä ulos ja luonnollisesti ulko-ovet on suojattava lukoilla. Ovien lukitsemista ja piilottamista ulkopuolisten katseilta edellytetään myös matkan aikana ajoneuvossa, hotellihuoneessa sekä organisaation toimitilojen katutasossa. Etätyöskentelyyn suositellaan etätyöskentelysopimusta työnantajan kanssa, jossa sovitaan myös mitä tietoa saa etäkoneelle tallentaa.

Ennen kaikkea käyttäjän ohjeistuksesta on huolehdittava ja siitä, että käyttäjä tietää vastuunsa.

Erityisen tärkeiksi vakuutusyhtiön tietoturvaluutta koskevat vaatimukset tekee se, että vakuutusyhtiö pystyy vahinkotilanteessa kieltäytymään korvausten maksusta, mikäli vaadittuja turvallisuusmäärityksiä ei ole noudatettu.

## *2.5 Vastuut*

Turvallinen tietojenkäsittely edellyttää myös erilaisten vastuualueiden määrittelyä. Esimerkiksi teknisen toteutuksen, seurannan ja varmuuskopioinnin vastuut on jaettava vastuuhenkilöille. Mikäli vastuuhenkilöiden toimenkuvat on määritelty epäselvästi, vastaan tulee jatkuvia ongelmia. (Miettinen 1999: 197.) Yksinkertaisena esimerkkinä voidaan ottaa vaikkapa varmuuskopiointi. Jos varmuuskopionauhan vaihtamisesta normaalisti vastaava henkilö on jostain syystä poissa, varmuuskopionauhan vaihtaminen jää muiden työntekijöiden vastuulle. Mikäli varahenkilöä ei ole määritelty, varmuuskopiointi todennäköisesti viivästyy tai unohtuu kokonaan. Vastaavien tapausten vuoksi vastuiden määrittely onkin erittäin tärkeää tietoturvaluuden ylläpitämiseksi.

Tässä tapauksessa, kun kyseessä on ulkoistettu tietohallinto, vastuiden määrittely on vielä tärkeämpää. Koska ylläpitäjä ei mitenkään voi ottaa kaikkea tietoturvaluuteen liittyvää vastuuta, on asiakasorganisaation valittava keskuudestaan vastuuhenkilöt hoitamaan jokapäiväisiä tietoturvaluuteen liittyviä rutiineja. Esimerkiksi hallinnollinen seuranta, jota käsitellään tämän luvun lopussa, ei onnistu ainoastaan ylläpitäjän toimesta. Jokaisen organisaation työntekijän on siis tunnettava oma vastuunsa tietoturvasta siinä missä omasta työstäänkin. Tämän vuoksi tietoturvapolitiikka sisältää kohdan, jossa vastuut määritellään.

Tietojärjestelmän vastuuhenkilöiden roolit jaetaan yleisesti neljään kategoriaan (Miettinen 1999: 197). Tässä tapauksessa roolit kuitenkin joudutaan selkeästi jakamaan ylläpitäjän ja asiakasorganisaation välillä. Pienemmässä organisaatiossa ei välttämättä ole luonnollisesti resursseja useiden vastuuhenkilöiden määrittelyyn. Monesti tämä on nimenomaan syynä toimintojen ulkoistamiselle.

Ensimmäinen yleinen tietojärjestelmän vastuuhenkilö on kehitys- vastuuhenkilö, joka vastaa koko tietojärjestelmän kehitykseen liittyvästä päätöksenteosta. Hänen tehtävänsä on ottaa kantaa koko loogisen järjestelmän tietoturvaluusasioihin ja esittää tietoturvaluusvaatimukset. Toinen laajempi rooli on tuotantovastuuhenkilö, joka vastaa järjestelmän tuotanto- ja käyttötoimintaan liittyvästä päätöksenteosta. Lisäksi tuotantovastuuhenkilö myöntää käyttö-

oikeudet käyttäjille. Hän vastaa niin ikään tietoturvallisuusvaatimusten määrittelystä ja muista loogisen järjestelmän sujuvuuteen liittyvistä päätöksistä. (Miettinen 1999: 197 - 198)

Kolmas tärkeä rooli on pääkäyttäjä, joka vastaa järjestelmän päivittäisestä ylläpidosta. Neljäs rooli on tietokoneen hoitaja, ”superuser”, joka on rooleista tärkein tietoturvallisuuden kehittämisessä ja ylläpidossa. (Miettinen 1999: 198 – 199.) Tietokoneen hoitaja on kuitenkin terminä nykypäivänä ehkä harvemmin käytetty ja vastaa tässä yhteydessä toimenkuvultaan pääkäyttäjää. Pääkäyttäjällä on paras laitteistotuntemus ja hän osaa tietoturvallisuuden ylläpitoon ja kehittämiseen liittyvät käytännön toimet. Pääkäyttäjä myös perustaa myönnettyt käyttäjätunnukset ja käyttöoikeudet.

Roolijakoon perustuen ulkoistettu ylläpito vastaakin tässä yhteydessä lähinnä pääkäyttäjän toimenkuvaa. Toimeksiantaja voi kuitenkin ottaa myös kehitysvastuuhenkilön roolin, mikäli asiakasorganisaatio niin tahtoo. Ylläpitäjä huolehtii nimensä mukaisesti tietojärjestelmän toiminnasta ja tietoturvasta teknisellä tasolla. Kehitys- ja tuotantovastuuhenkilöiden roolit jäävät näin ollen asiakasorganisaation vastuulle. Asiakasorganisaatio huolehtii järjestelmän kehittämiseen liittyvistä päätöksistä, jotka ylläpitäjä toteuttaa. Lisäksi asiakasorganisaation on luonnollisesti huolehdittava työntekijöidensä tietoturvallisesta toiminnasta ja tarpeen mukaan informoida ylläpitäjää ongelmista, joihin teknisellä toteutuksella voidaan puuttua.

Vastuualueiden määrittely on tärkeää nimenomaan sen vuoksi, että ongelman ilmetessä voidaan selvittää kenen vastuualueelle ongelma kuuluu ja näin päättää esimerkiksi mahdollisesta korvausvelvollisuudesta. Näin vältetään lisäksi turhalta syytelyltä, joka saattaisi riitauttaa ylläpitosopimuksen osapuolet.

## **2.6 Riskianalyysi**

Riskianalyysi on tehokas työkalu organisaation tietoturvallisuuden parantamiseksi. Se on ensimmäinen tehtävä mihin panostetaan kun lähdetään luomaan organisaatiolle tietoturvaratkaisua. ISO/IEC 17799 –standardin ensimmäinen pääkohta käsittelee riskien analysointia ja evaluointia. (Hakala ym. 2006: 47)

Riskianalyysi voidaan jakaa kahteen osa-alueeseen, riskikartoitukseen ja riskien arviointiin. Riskikartoituksen avulla etsitään organisaation toimintaa uhkaavat riskit. Riskejä arvioimalla pyritään selvittämään löydettyjen riskien vaikutus organisaation toimintaan. Yleinen riskikartoitus tehdään ennen varsinaista organisaatioon kohdistuvaa riskikartoitusta. Sen tarkoituksena on löytää yleisimmät tietojenkäsittelyyn liittyvät riskit riippumatta organisaatiosta.

Yleistä riskikartoitusta voidaan käyttää oppaana organisaation riskejä kartoitettaessa, eli tehtäessä tietojärjestelmäkohtaista riskikartoitusta. Tietojärjestelmäkohtaisen riskikartoituksen jälkeen tehdään riskien arviointi, eli tutkitaan riskien vaikutukset organisaation toimintaan ja niiden toteutumisen todennäköisyys. Näin saadaan selville riskit joihin on ehdottomasti varauduttava, sekä ne riskit jotka eivät välttämättä vaadi varautumista. (Hakala ym. 2006: 80 - 82)

## ***2.7 Koulutus ja ohjeistus***

Aiemmin mainittu Ernst & Youngin tietoturvaselvitys kertoo myös, että vaikka yritykset pitävät tietoturvatietoisuuden puutetta riskinä, vain 28 %:lla haastatelluista yrityksistä tietoturvatietoisuuden kehittäminen on ollut keskeinen kehityshanke vuonna 2004. Tietoturva-asiantuntija Ari Väisänen kertoo selvityksen osoittavan, että organisaatiot keskittyvät suurimmilta osin ulkopuolisiin riskeihin, vaikka todellisuudessa suurimmat riskit ovat peräisin organisaatioiden sisältä. (Ernst & Young: Tietoturvariskejä... 2004)

Tietoturvallisuuskoulutus on yksinkertainen keino saattaa tietoturvallisuuden vaatimukset henkilöstön tietoon ja opastaa tietoturvallisuuden vaatimien menetelmien käytössä. Koulutuksen on hyvä tuoda ilmi tietoturvallisuuden merkitys organisaation toiminnalle, tietoturvallisuuden peruskäsitteet ja osa-alueet, vastuut organisaatiossa, tietoturvallisuus työntekijän ympäristössä kuten työasemilla, verkkoresursseissa ja etäkäytössä. Lisäksi sen tulee käsitellä raportointiohjeet ongelmatapauksissa sekä yrityksen yhteyshenkilöt, joiden puoleen tietoturvallisuusasioissa tulee kääntyä. Tärkeää on myös kertoa, mistä työntekijä voi saada lisäohjeistusta, esimerkiksi yrityksen verkossa sijaitsevat tietoturvaohjeet. (Miettinen 1999: 158 - 159)

Opinnäytetyön tapauksessa asiakasorganisaatio ei välttämättä pysty suorittamaan tietoturvallisuuskoulutusta täysipainoisesti itse, johtuen tietoturvan teknisen toteutuksen ulkoistamisesta. Toimeksiantajalla on kuitenkin tarvittaessa varmasti kyky lähteä mukaan tietoturvallisuuskoulutuksen järjestämiseen. Näin ollen tietoturvallisuuskoulutuksen voisi järjestää niin, että asiakasorganisaatio kertoo tietoturvallisuuden merkityksestä organisaation näkökulmasta. Tietoturvan yleisperiaatteet ja teknisen ohjeistuksen voisi suorittaa toimeksiantaja. Asiakasorganisaation avainhenkilöille, kuten esimerkiksi varmuuskopioinnista vastaaville työntekijöille, on lisäksi syytä järjestää henkilö- tai ryhmäkohtainen koulutus. Koulutuksessa varmuuskopioinnin vaatimat toimenpiteet käydään läpi yksityiskohtaisesti ja esimerkkiä näyttämällä. Näin työntekijän virhemahdollisuudet kriittisissä toimenpiteissä saadaan minimoitua.

Tietoturvallisten toimintatapojen ohjeistus henkilöstölle on koulutuksen ohella ensisijainen tapa minimoida toimintaa uhkaavat inhimilliset riskit. Toimintatapojen ohjeistus on saatettava kaikkien työntekijöiden tietoon ja vaivattomasti saataville. Esimerkiksi yrityksen jaettu verkkokansio on järkevä paikka ohjeistuksen säilyttämiselle, jolloin työntekijä saa tarpeen tullen ohjeet nopeasti käsiinsä. Ohjeistuksen luonnissa on syytä kuitenkin välttää sääntömäisyyttä, sillä määräys menettelytavasta ja uhkaus rangaistuksesta ei motivoi käyttäjää. Hyvässä ohjeistuksessa vaaditut menettelytavat on perusteltu sekä organisaation että työntekijän näkökulmasta. (Hakala ym. 2006: 103)

## ***2.8 Vaitiolovelvollisuus***

Organisaation ja työntekijän välinen salassapitosopimus on henkilöstöturvallisuuden perustavanlaatuinen sopimus. Samaa tarkoitusta ajavat organisaatioiden väliset salassapitosopimukset. Sopimus on juridisesti sitova asiakirja, joka on voimassa yhteistyön päättämisen jälkeenkin. Tästä syystä sopimuksen ehdot on mietittävä tarkasti ennen allekirjoittamista. Salassapitosopimus on ensisijainen tapa yrityksen luottamuksellisten tietojen suojaamiseksi. Sopimus määrittelee allekirjoittavan osapuolen velvollisuudet tiedon salassa pitämisestä sekä mahdollisen rikkomuksen aiheuttamat rangaistukset. Kun osapuolten välillä vaihdetaan luottamuksellista tietoa, on ehdottomasti harkittava salassapitosopimuksen käyttöä. Yritykselle se on myös juridinen turva mahdollisen rikkomuksen paljastuessa. Organisaation ja työntekijän kesken solmittava salassapitosopimus velvoittaa myös työntekijän sitoutumaan organisaatioon, joten oikein muotoiltu salassapitosopimus parantaa osaltaan myös työntekijöiden sitoutumista organisaation tietoturvalliseen toimintaan. (Miettinen 1999: 165 - 167)

## ***2.9 Hallinnollinen seuranta***

Kuten on usein todettu, tietoturvallisuuden vaaratekijät ovat yleisimmin peräisin ihmisten toiminnasta, inhimillisistä virheistä, kiireestä tai huolimattomuudesta. Organisaation työntekijöiden asennoitumisen, työmenetelmien ja tietoturvaluustietouden tekninen seuraaminen ei ole käytännössä mahdollista. Se vaatii niin organisaation hallinnolta kuin jokaiselta työntekijältäkin havainnointia ja ongelmien raportointia. (Hakala ym. 2006: 102)

Päävastuu henkilöstön toiminnasta on tässä tapauksessa luonnollisesti asiakasorganisaatiolla. Asiakasorganisaation hallinto ei missään tapauksessa saa laiminlyödä henkilöstönsä toiminnan tietoturvallisuuden seuranta. Tämän vuoksi tietoturvapoliittikkaan kuuluu kohta, joka velvoittaa organisaation jokaisen työntekijän raportoimaan havaitsemistaan ongelmista ja tietoturvallisuuden

loukkauksista. Täytyy kuitenkin muistaa, että kyseinen asia on tiedotettava ymmärrettävästi kaikille työntekijöille, jotta jokainen ymmärtää vastuunsa yrityksen tietoturvaketjun lenkkinä. Kun työntekijä ymmärtää oman tärkeytensä ja paikkansa organisaatiossa, auttaa se motivoimaan työntekijää toimimaan yrityksen etujen mukaisesti.

### 3 Henkilöstöturvallisuus

Kiteytettynä henkilöstöturvallisuus tarkoittaa yrityksen tietojen ja tietojenkäsittelyn suojaamista ihmisten tahallisilta ja tahattomilta uhilta, sekä ihmisten toimintaa tietoturvallisuuden varmistajana. (Miettinen 1999: 18)

Toisin sanoen henkilöstöturvallisuuden tavoitteena on varmistaa järjestelmän käyttäjille tarvittavat mahdollisuudet työtehtävien suorittamiseen, sekä rajoittaa järjestelmän käyttöoikeuksia tarpeettomilta osin. (Hakala ym. 2006: 11)

Aiemmin on jo todettu, että organisaation henkilöstö muodostaa suurimman tietoturvallisuusriskin. Keskeisiä riskejä ovat henkilön soveltuvuus työtehtäviin, tiedonsaanti- ja käyttöoikeuksien asianmukainen määrittely, sekä riittävä turvallisuuskoulutus ja valvonta. Riskejä voidaan lieventää huolellisesti hoidetulla henkilöstöturvallisuudella. (Rousku 2003: 54 – 56)

Tässä luvussa pyritään siis käsittelemään niitä asioita, jotka tulee ottaa huomioon suunniteltaessa henkilöstölle turvallista tietojärjestelmää sekä miten voidaan estää yrityksen sisältä kohdistuvien uhkien muodostuminen. Tässä luvussa tutustutaan henkilöstön käyttöoikeuksiin ja –rajoituksiin sekä tietoturvaan vaikuttaviin tekijöihin paikallisen työaseman, sisäverkon, etäkäytön ja kannettavien tietokoneiden, datan tallentamisen sekä tallennusmedioiden kanalta. Lisäksi käsitellään Internet –käyttöpolitiikkaa, sähköpostiviestinnän suojaamiseen liittyviä asioita, sekä käyttäjätilejä ja salasanoja.

#### 3.1 Paikallinen työasema

Käyttäjän osaaminen ja motivaatio ovat avainasemassa puhuttaessa työaseman käytön turvallisuudesta. Tämän vuoksi organisaation täytyy huolehtia siitä, että käyttäjää ohjeistetaan tarpeen mukaan työaseman ja verkkoresurssien oikeaoppisesta käytöstä. (Hakala ym. 2006: 124)

Työasemien turvaamisessa huomioon otettavia uhkia ovat ensisijaisesti tallennettujen tietojen paljastuminen, tiedon tahallinen tai tahaton eheyden muutos sekä tiedon saatavuuden estyminen työasemassa tai verkossa. Tällöin on mahdollista, että tietoja on vahingoitettu, poistettu, tietojen tai palveluiden käyttö on estetty tai käsittelykapasiteettia vahingoitettu tai ylikuormitettu. Syynä tähän on useimmiten koneelle päässyt luvaton käyttäjä, liian laajat käyttöoikeudet tai tietojen suojaamaton lähettäminen verkon yli. (Allen 2002: 23 - 25)

Näihin ongelmiin varautumiseen keskeiset menetelmät ovat käyttäjätilien muokkaaminen työtehtäviä vastaavaksi ja käyttäjän opastaminen oikeaoppiseen toimintaan. Käyttäjätilejä käsitellään tarkemmin myöhemmin henkilöstöturvallisuutta koskevassa luvussa. Käyttäjän opastamista on aiemmin käsitelty hallinnollisen turvallisuuden koulutusta ja ohjeistusta koskevassa luvussa. Tietojen oikeaoppista lähettämistä verkon yli käsitellään tarkemmin sähköpostia koskevassa luvussa.

Olellaisia ongelmia käyttäjän toiminnassa voivat olla esimerkiksi työaseman jättäminen lukitsematta ja ilman valvontaa, tai käyttäjätunnuksen ja salasanan paljastuminen luvottomalle käyttäjälle. Ainoa tapa vaikuttaa tähän asiaan, on kertoa käyttäjälle miksi työasema pitää lukita ja miksi käyttäjätunnusta ja salasanaa ei saa esimerkiksi kirjoittaa näytön kulmaan kiinnitetylle tarralapulle. Nämä ovat asioita jotka tulee muistaa käydä läpi tietoturvallisuuskoulutuksessa ja -ohjeistuksessa. Olellaista on, että käyttäjää opastettaessa ei kerrota ainoastaan miten, vaan myös miksi. (Hakala ym. 2006: 103)

### **3.2 Sisäverkko**

Organisaation sisäisessä verkossa käyttäjien oikeusmäärittelyt koskevat lähinnä tiedostonjako- ja tulostuspalveluita. Tulostuspalvelut on viisasta jakaa kaikkien käyttäjien saataville, niin että yhden tulostimen vikaantuessa käyttäjä voi valita toisen tulostimen, jolla jatkaa työntekoaan.

Tiedostopalveluiden käyttöoikeudet on puolestaan syytä määritellä käyttäjän työtehtävien mukaisesti, niin ettei kaikilla suinkaan ole pääsyä jokaiseen kansioon. Esimerkiksi jos markkinointiosaston työntekijä pääsee ilman pätevää syytä käsiksi taloushallinnon tiedostoihin, on olemassa riski, että hän tuhoaa tai vioittaa tahallisesti tai tahattomasti tietoja jotka eivät kuulu hänen työtehtäviensä piiriin. Jokaisella käyttäjällä tulee kuitenkin olla pääsy niihin tietoihin joita hän tarvitsee työnsä suorittamiseksi. Tiedostojen käyttöoikeudet tulee määritellä niin, että käyttäjällä on enimmillään oikeus lukea, suorittaa, tallentaa tai poistaa tiedostoja. Käyttöoikeuksien muuttamiseen ei loppukäyttäjälle anneta oikeutta. (Hakala ym. 2006: 162)

### **3.3 Etäkäyttö ja kannettavat tietokoneet**

Etäkäyttö aiheuttaa suuren haasteen organisaation tietoturvallisuudelle, sillä etätyössä käytettävää työasemaa käytetään muissakin järjestelmissä kuin organisaation sisäisessä järjestelmässä. Virustorjunnan kannalta tilanne on hankala, sillä jos kone on saanut tartunnan toisessa verkossa, saattaa virus levitä organisaation verk-



koon. Mikäli etäkäyttöön käytetään kannettavaa tietokonetta, virustietokannat eivät välttämättä ole päivittyneet asianmukaisesti sillä aikaa kun kone on ollut kytkettynä vieraaseen järjestelmään. Näin ollen virustartunnan riski kasvaa. Mikäli yrityksen työntekijöillä on tarvetta etäkäyttöön, yleinen suositus ja toimeksiantajan käytäntö on, että siihen käytetään organisaation toimittamaa kannettavaa tietokonetta. Näin kotikoneen haavoittuvuudet eivät heikennä organisaation tietoturvallisuutta. Kannettaviin tietokoneisiin asennetaan virustorjuntaohjelmiston lisäksi palomuuriohjelmisto, sillä ulkopuolisessa verkossa ne eivät pääse luonnollisesti-kaan hyödyntämään organisaation omaa palomuuria. (Hakala ym. 2006: 137)

Kannettavan tietokoneen käytössä on otettava huomioon myös fyysinen tietoturva. Tietokone on usein liikkeellä organisaation ulkopuolella ja on näin erityisesti alttiina varkauksille ja väärinkäytöksille. Varoittavia esimerkkejä yleisellä paikalla auton takapenkiltä varastetuista kannettavista tietokoneista riittää. Fyysistä turvallisuutta parantavat turvamerkinnot, joita käsitellään tarkemmin fyysistä tietoturvaä käsittelyssä luvussa. Koneen sisältämän tiedon suojaamiseen yksi varteenotettava ja toimeksiantajallakin paljon käytetty menetelmä on käynnistysalustana, jolla kannettavat tietokoneet kannattaa aina suojata. Samoin kaikki muut organisaation ulkopuolella käytettävät tietokoneet. Mikäli tietokone joutuu väärin käsiin, käynnistysalustana estää tai ainakin hidastaa merkittävästi ulkopuolisen henkilön pääsyä koneelle.

Ongelman ratkaisuna voidaan käyttää myös kiintolevyn salausta asianmukaisella ohjelmistolla kokonaan tai hakemisto-/tiedostokohtaisesti. Joissakin kannettavissa tietokoneissa laitteistopohjainen salaus mahdollistaa tiedon salauksen esimerkiksi älykortilla annettavalla salausavaimella. Tätä menetelmää käytettäessä on viisasta mahdollistaa saatavuus myös toisella salausavaimella, jolloin pääavaimen kadotessa tieto saadaan talteen toisella avaimella. (Hakala ym. 2006: 137 - 138)

### **3.3.1 VPN (Virtual Private Network)**

Suunniteltaessa etäkäyttöä tietoliikenne täytyy toteuttaa niin että organisaation ulkopuolella voidaan turvallisesti työskennellä ja käyttää yrityksen verkkoresurseja. Tietoliikenne tulee siis asianmukaisesti salata. Salaus suoritetaan yleisimmin käyttämällä VPN-tekniikkaa (Virtual Private Network). (Hakala ym. 2006: 137)

VPN-tekniikkaa käyttämällä organisaation verkon ja etäkäyttäjän välinen liikenne suojataan rakentamalla ns. tunneli verkon etäkäyttöpalvelimen ja käyttäjän tietokoneen välille. VPN-asiakas ottaa yhteyden VPN-palvelimelle joka hyväksyy yhteyden ja tarjoaa

pääsyn valtuutettuihin verkkoresursseihin. Tieto kapsuloidaan, eli pakataan ja salataan tunnelissa. Nykyaikaiset VPN-yhteydet käyttävät vahvaa salausta ja käyttäjätunnistusta. VPN-yhteyden rakentamiseen käytettävät protokollat ovat riippuvaisia käytettävästä alustasta, eikä niiden yksityiskohtaisempi käsitteleminen ole tässä yhteydessä olennaista. (Hakala ym. 2006: 284 - 293)

### 3.3.2 WLAN (Wireless Local Area Network)

Kannettavia tietokoneita käyttävissä yrityksissä on myös nykypäivänä huomattavasti yleistynyt langattomien verkkojen käyttö. Syynä tähän on yksinkertaisesti käytön helppous. Langattoman yhteyden muodostamiseen kykenevällä kannettavalla tietokoneella verkkoon kirjautuminen käy verkon peittoalueella sijainnista riippumatta ja ilman verkkokaapelia. Langattomat verkot vaativat toisenlaista suojausta kuin yrityksen runkoverkko, sillä ne käyttävät kaapeleiden sijaan radiosignaaleita ja ovat erityisen alttiita tietoturvaloukkauksille, kuten vakoilulle ja verkkoresurssien luvattomalle käytölle. Langattoman verkon perussuojaus on heikko, joten yritykset käyttävät usein VPN-tekniikkaa liikenteen suojaamiseksi. Langattoma verkkoa suunniteltaessa kannattaa miettiä kuinka paljon voimavaroja salauksen toteuttamiseen todella halutaan käyttää. Verkon peittoalue on myös otettava huomioon ja mietittävä mihin palveluihin verkon kautta voidaan sallia pääsy. Mikäli verkon peittoalue ei riitä organisaation julkisiin tiloihin, voidaan verkkoa käyttää melko huolettomasti. Tämä lieneekin paras keino välttyä vakoilulta tai yrityksen Internet-yhteyden luvattomalta käytöltä. (Hakala ym. 2006: 293 - 298)

Langattoman liikenteen suojaamiseksi ja luvattoman käytön estämiseksi on kehitetty erilaisia suojausmenetelmiä, mutta niiden käsittely yksityiskohtaisesti ei ole olennaista tässä yhteydessä. Tarkemmin WLAN-tietoturvasta voi lukea Tuire Vähä-Tourun opinäytetyöstä ”Langattoman lähiverkon toteutus” ja sen luvusta 3, ”WLAN ja tietoturva”.

### 3.4 Datan tallentaminen

Datan tallentamisen tulee aina tapahtua turvallisesti, niin että datan varmistaminen onnistuu ongelmitta. Yleinen ja hyväksi havaittu käytäntö on tallentaa työasemilla tuotettu data tiedostopalvelimelle käyttäjän omaan hakemistoon, jolloin datan varmistaminen onnistuu keskitetysti palvelimelta varmuuskopiointiohjelmiston avulla. Mikäli kuitenkin halutaan tallentaa dataa työasemille, tulisi varmistus hoitaa niin, että työasema tallentaa sammutuksen tai käynnistyksen yhteydessä automaattisesti sisältämänsä datan palvelimelle. Näin toteutettuna datan varmistaminen onnistuu aina keskitetysti palvelimelta. Organisaation tulee huolehtia että käyttäjiä oh-

jeistetaan ymmärrettävästi datan halutusta tallennuspaikasta, näin minimoidaan tiedon häviämisen riski esimerkiksi työaseman kiintolevyn rikkoutuessa. Missään tapauksessa ei datan varmistamista saa jättää yksin käyttäjien harteille. (Hakala ym. 2006: 135)

### ***3.5 Tallennusmediat***

Yhden nykypäivänä vähemmälle huomiolle jääneen tietoturvarisikin muodostavat siirrettävät tallennusmediat, kuten CD-R/RW, levyke, ulkoinen kiintolevy tai USB-massamuistilaitte. 90-luvulla saastuneet levykkeet olivat yksi keskeinen virusten leviämistapa. Nykyään levykkeiden käyttö on osittain korvattu CD-R/RW –levyillä ja USB-massamuistilaitteilla. Jostain syystä lähdekirjallisuudessa ei juurikaan huomioida ulkoisten tallennusmedioiden käyttöä. Nykypäivänä esimerkiksi kannettavat MP3-soittimet ovat erittäin yleisiä ja antavat työntekijöille mahdollisuuden kuljettaa musiikkia mukanaan kotoa töihin tai päinvastoin. Näin mahdollisesti kotikoneeseen tarttunut virus pesiytyy myös MP3-soittimeen, jonka mukana se kulkeutuu työpaikan verkkoon.

Tämä koskee luonnollisesti kaikkia siirrettäviä tallennusmedioita joita kuljetetaan mukana organisaation ja muiden tietojärjestelmien välillä. Tulee aina muistaa että organisaation sisällä ei saa käyttää samoja tallennusmedioita kuin esimerkiksi kotikoneissa jotka ovat monesti yritysverkkoa enemmän alttiina haittaohjelmille ja viruksille. Monissa yrityksissä kannettavat muistivälineet ovat välttämättömyys kuljettaessa dataa organisaatioiden välillä. Tässä asiassa kannattaa kuitenkin ehdottomasti käyttää tarkkaa harkintaa ja maalaisjärkeä, sillä ihan jokaiseen koneeseen ei kannettavaa muistivälinettä kannata laittaa. Siirrettäviin tallennusmedioihin kannattaa rinnastaa samanlaista lähestymistapaa kuin kannettavien tietokoneiden turvaamiseen, jota käsiteltiin etäkäyttöä koskevassa luvussa.

### ***3.6 Internetin käyttö***

Internet on maailmanlaajuinen julkinen verkko, jonka käyttö onnistuu keneltä tahansa, jolla on Internet-yhteys. Luonnollisesti Internetiä käyttää kirjava joukko ihmisiä, joiden kaikkien tarkoitusten oikeellisuudesta ei voi antaa mitään takuita. Näin ollen tietojärjestelmän suojaaminen Internetin tuomilta uhilta on elintärkeää. Tietoverkon tekniseen suojaamiseen paneudutaan tässä opinnäytetyössä tietoliikenneturvallisuutta koskevassa luvussa. Henkilöstöturvallisuuden kannalta Internet muodostaa toisenlaisen uhan, joka liittyy käyttäjien toimintaan.

Organisaation on tietoturvallisuuskoulutuksen ja -ohjeistuksen avulla tärkeää puuttua käyttäjien toimintatapoihin Internetissä ja

varmistaa että jokainen työntekijä tietää Internetin riskeistä. Työntekijä voi omalla huolellisella toiminnallaan parantaa huomattavasti Internetin tietoturvallisuutta. Näin organisaatiossa käsiteltävät tiedot eivät joudu ulkopuolisten tietoon. (Miettinen 1999: 219)

Internetin käytössä työntekijän on hyvä huomioida ensinnäkin Internetin tietojen oikeellisuus. Koska Internetin käyttäjäkunta on kirjava, tulee aina varmistua Internetistä saatujen tietojen oikeellisuudesta. Kuka tahansa käyttäjä voi lisätä Internetiin tahattomasti tai tahallisesti tietoa joka ei pidä paikkaansa, tai suoranaisesti joutaa harhaan. Mikäli siis tietojen oikeellisuutta ei voida varmistaa, ei tietoa kannata myöskään käyttää hyväksi. (Miettinen 1999: 220)

Esimerkkinä tästä voidaan ottaa vaikkapa suosittu käyttäjien ylläpitämä verkkotietosanakirja Wikipedia (<http://fi.wikipedia.org/>). Kyseessä on siis vapaasti muokattava tietosanakirja, johon kuka tahansa voi lähettää tietoa. Juuri tästä syystä Wikipediaa ei voida käyttää esimerkiksi tämän opinnäytetyön lähdeaineistona. Muuten Wikipedia sisältää kuitenkin erittäin hyödyllistä ja suurimmaksi osaksi oikeellista tietoa. Wikipedian vastapainoksi on kuitenkin kehitetty Hikipedia (<http://hiki.pedia.ws/>), joka on käyttäjien ylläpitämä ”luulosanakirja”. Ulkoasultaan molemmat näyttävät huomattavan paljon samanlaisilta, joten käyttäjien on oltava tarkkana. Hakutiedoista esimerkkinä voidaan ottaa vaikkapa ”Bill Gates”. Wikipedian mukaan ”Bill Gates on toinen Microsoft-ohjelmistoyhtiön perustajista”. Hikipedia vastaa hakuun kertomalla että ”Bill Gates on pelätyin diktaattori jälkeen Stalinin”. Oikeasta tiedosta ei liene epäilystäkään. Tämä on oleellinen esimerkki Internetin tietojen oikeellisuudesta.

Toisekseen verkossa jaettavien ohjelmien asentaminen on erittäin kyseenalaista. Niidenkään alkuperästä ei välttämättä saada varmaa tietoa ja jotkin ohjelmat saattavatkin sisältää ns. ”haittaohjelmia”. Asennettaessa ne voivat toimia moitteettomasti, mutta niiden mukana voi mahdollisesti olla viruksia tai muita haitallisia ohjelmia, jotka saattavat esimerkiksi kerätä tietoa työasemasta ja lähettää sitä ulkopuolisille. Mikäli kyseessä on virus, se saattaa asentamisen jälkeen haitata työaseman käyttöä, tai jopa loukata tietojen eheyttä ja käytettävyyttä. Tämän ongelman ratkaisuksi onkin hyvä ylläpitäjän toimesta ohjelmallisesti kieltää tavallisia käyttäjiä asentamasta työasemalleen ohjelmistoja, ellei niiden asentaminen ole täysin välttämätöntä. Mikäli käyttäjä kuitenkin lataa tietoa Internetistä työasemalleen, on hyvä suorittaa sille virustarkistus. Reaaliaikainen virustarkistus on myös ylläpitäjältä viisas ja yleisesti käytetty ratkaisu, niin että aina kun verkosta ladataan tietoa, virustorjuntaohjelma tarkistaa sen sisällön ja ilmoittaa mahdollisesta haitallisesta sisällöstä. Käyttäjän toiminta on kuitenkin avainasemassa, sillä uusia haittaohjelmia ja viruksia ilmestyy päivittäin. Näin ollen vi-

rustutka ei aina välttämättä pysty tunnistamaan kaikkea haitallista sisältöä. (Miettinen 1999: 220)

Kolmantena tulee ottaa huomioon arkaluonteisen tiedon lähettäminen Internetissä. Koska Internet-verkossa viestintä tapahtuu selväkielisenä, sitä on helppo salakuunnella. Näin ollen organisaation luottamuksellinen tieto on vaarassa paljastua. Arkaluonteista tietoa ei siis koskaan kannata lähettää Internetin välityksellä, ellei asianmukaista suojausta pystytä toteuttamaan. Mikäli luottamuksellista tietoa on välttämätöntä lähettää Internetin välityksellä, organisaation tulee huolehtia vaadittujen salausten menetelmien käytön ohjeistuksesta käyttäjälle. (Miettinen 1999: 220)

### 3.7 Sähköposti

Lähtökohtaisesti jokaiselle asiakasorganisaatiolle asennetaan oma sähköpostipalvelin. Palvelimien suojaamista käsitellään myöhemmin tietoliikenneturvallisuuksessa koskevassa luvussa ja samoja asioita sovelletaan myös sähköpostipalvelimen suojaamiseen.

Sähköpostiviestintä hyödyntää pääasiassa kolmea protokollaa. IMAP (Internet Message Access Protocol) on sähköpostin lukemiseen tarkoitettu protokolla, jota käytetään silloin kun halutaan antaa käyttäjille mahdollisuus lukea sähköpostiaan selaimen kautta. IMAP antaa mahdollisuuden lukea sähköpostia palvelimelta, muttei lataa sitä itse työasemalle. (Wikipedia 2007: IMAP)

POP3 (Post Office Protocol version 3) on sähköpostin hakemiseen tarkoitettu protokolla. Tätä protokollaa käytetään kun halutaan hakea sähköpostiviestit palvelimelta työasemalle. (Wikipedia 2007: POP3.) SMTP (Simple Mail Transfer Protocol) puolestaan on sähköpostiviestin lähettämiseen ja vastaanottamiseen tarkoitettu protokolla, joka huolehtii sähköpostin toimituksesta ja vastaanottamisesta (Wikipedia 2007: SMTP). Valinta IMAP- ja POP3-protokollien välillä on täysin riippuvainen organisaation tarpeista. Tietoturvallisuuden kannalta molemmissa on otettava huomioon samat asiat.

Sähköpostiviestinnän tekninen tarkastelu ei tässä yhteydessä ole kuitenkaan olennaisin asia. Tärkein asia organisaation turvallisessa viestinnässä liittyy käyttäjien toimintaan ja viestinnän salaamiseen, joten niihin keskitytään tässä luvussa.

#### 3.7.1 Käyttäjien ohjeistus

Sähköpostin suojaamisen lähtökohdaksi on tärkeää luoda työntekijöille organisaation sähköpostin käyttöä varten selkokieli ohjeistus. Koska lainsäädännön mukaan työntekijöiden sähkö-

postiviestintää ei saa ”vakoilla”, on tärkeintä että työntekijä itse ottaa vastuun toiminnastaan sähköpostiviestintään liittyen. (Miettinen 1999: 207)

Sähköpostin käyttöön liittyvän ohjeistuksen tulee sisältää selkokielisesti riskit joita sähköpostin käyttöön liittyy. Riskeistä olennaisin on ehkä se, että viestintä tapahtuu pääasiassa selväkielisenä yleisen verkon läpi. Tällöin viestinnän ”salakuuntelu” on mahdollista. Sähköpostin välityksellä tietokoneeseen saattaa myös tarttua ns. ”vihamielisiä” ohjelmia, eli haittaohjelmia tai viruksia. Roskapostin mahdollisuutta ei myöskään voida unohtaa. (Miettinen 1999: 206)

Kun käyttäjä ymmärtää sähköpostiliikenteen riskit, on huomattavasti helpompi perustella sähköpostin käyttöön liittyvät määräykset. Asioita joita tulee ohjeistuksessa huomioida, on ensimmäiseksi oikean sähköpostiosoitteen valinta. Lähetettäessä tulee varmistua vastaanottajasta ja osoitteesta, niin ettei viesti työntekijän huolimattomuudesta johtuen päädy väärälle vastaanottajalle. Jakelulistoja tulee myös päivittää sitä mukaa kun tiedetään siinä olevien osoitteiden muuttuneen tai poistuneen käytöstä. Sähköpostilaatikon säännöllinen siivoaminen on myös oleellista. Viestien arkistointi puolestaan vie tilaa ja hidastaa sähköpostin käyttöä. Näin ollen ne viestit jotka eivät vaadi arkistointia, tulee poistaa säännöllisesti. Arkaluontoisen tiedon lähettämistä tulee ehdottomasti välttää. Mikäli sitä on kuitenkin välttämätöntä lähettää, salauksesta tulee huolehtia. Roskapostin ilmaantuessa sähköpostilaatikkoon on välittömästi ryhdyttävä toimenpiteisiin sen ehkäisemiseksi. (Miettinen 1999: 206)

Lisäksi vastaanotettaessa liitetiedostoja, ne on aina tarkistettava virustorjuntaohjelmalla. Tässä tapauksessa tosin lähdetään siitä oletuksesta, että virustorjuntaohjelma seuraa automaattisesti sähköpostiliikennettä ja tarkastaa myös liitetiedostot. Epäilyttäviä liitetiedostoja ei luonnollisestikaan saa avata, mikäli sellaisia sähköpostilaatikkoon ilmaantuu. Ylläpitäjä voi tässä asiassa vaikuttaa liitetiedostoihin suodattamalla sähköpostipalvelimelta ei-toivotut liitetiedostot, esimerkiksi tietyssä tiedostomuodossa olevat liitteet joiden tiedetään olevan haitallisia tai todennäköisesti sisältävän haitallisia ohjelmia. Lisäksi voidaan suodattaa myös liian suuret liitetiedostot jotka kuormittavat organisaation tietoverkkoa huomattavasti. Tästä on kuitenkin muistettava kertoa työntekijöille ja yhteistyökumppaneille tietojen menettämisen välttämiseksi. (Miettinen 1999: 206)

On luonnollista että yksityisposti on erotettava työpostista, joskin postin valvonta on lain puitteissa ongelma. Väärinkäytösepäilyisäkään ei saa käyttää työntekijän yksityisyyttä loukkaavaa valvon-

taa. Työnantajalla on oikeus kieltää sähköpostin käyttäminen yksityisiin tarkoituksiin, mutta toinen asia on, onko kiellosta enemmän hyötyä kuin haittaa. Mikäli halutaan antaa työntekijöille mahdollisuus yksityisen sähköpostin käyttämiseen, kannattaa kannustaa heitä käyttämään webmail-tilejä. Tietenkin tämän tulee tapahtua työajan ulkopuolella. Yksityisposti on kuitenkin aina riski, sillä myös se saattaa sisältää epäilyttävää materiaalia, kuten esimerkiksi roskapostin mukana leviäviä haittaohjelmia. (Järvinen 2003: 251 - 252)

Työntekijän työsuhteen päättyessä asiakasorganisaatio on luonnollisesti ilmoitusvelvollinen poistuneen työntekijän sähköpostiosoitteen ilmoittamisesta ylläpitäjälle. Tällöin ylläpitäjä voi viipymättä poistaa tarpeettomaksi käyneen sähköpostiosoitteen, joka väärinkäyttönä voisi johtaa hankaluuksiin.

Erityisesti on muistettava että ylläpitäjäkin on vastuussa salassapidosta. Vaikka ylläpitäjä ei näkisi viestien sisältöä, sähköpostipalvelimen lokitiedotkin ovat luottamuksellista aineistoa. Näin ollen ylläpitäjän on pidettävä tiedot salassa oikeudellisten seuraamusten uhalla. (Järvinen 2003: 250 - 251)

Nämä asiat on siis syytä ottaa huomioon työntekijöiden sähköpostikoulutuksessa ja -ohjeistuksessa. Ehdottomasti on korostettava työntekijän omaa vastuuta sähköpostin käytöstä, sillä hän on lopputelissä se joka vastaa oman viestintänsä turvallisuudesta ja on näin ollen osaltaan vastuussa organisaation tietoturvasuodattamisesta.

### 3.7.2 Roskaposti

Roskaposti on nykypäivänä ehkä yksi puhutuimmista tietoverkon kirouksista. Tutkimuksen mukaan syksyllä 2006 jopa 90 % postiliikenteestä oli viestejä, jotka saapuivat vastaanottajalleen pyytämättä. Toimeksiantajallakin on käytössään roskapostin suodatus ja yleisesti käytettävissä F-Secure Client Security -ohjelmistoissa on myös roskapostin suodatus. Tosiasia kuitenkin on ettei yksikään suodatin voi täydellä varmuudella estää roskapostia ja roskaposti kuluttaa joka tapauksessa verkon resursseja vaikka se suodattimeen jäisikin. Suodatinta voi toki säätää koko ajan suodattamaan enemmän postia tiukemmilla kriteereillä, mutta jossain vaiheessa vastaan tulee väkisinkin se tilanne, ettei asiallinenkaan posti enää pääse läpi roskapostisuodattimesta. Lisäksi Suomessa on voimassa erittäin tiukka sähköisen viestinnän tietosuojalaki joka edellyttää, että mikäli roskapostia poistetaan automaattisesti, siihen on oltava kirjallinen lupa työntekijältä. Näin ollen tässä asiassa paras keino onkin ottaa käyttöön vanha kunnon maalaisjärki. (Järvinen 2007: 40 - 41)

Kaikista tehokkain keino onkin paneutua siihen, mitä on loppukäyttäjän korvien välissä. Kattava sähköpostiohjeistus voi siis olla paras tapa suojautua roskapostilta. Seuraavat ohjeet on poimittu Petteri Järvisen kirjoittamasta Tietokone-lehdessä julkaistusta artikkelista ja muokattu opinnäytetyön tarkoituksiin sopiviksi. Vaikkakin ohjeet on alunperin tarkoitettu yksityishenkilöille, niitä kannattaa ehdottomasti soveltaa tehtäessä sähköpostiohjeistusta organisaation loppukäyttäjille:

1. *Suojele osoitettasi.* Sähköpostiosoitetta ei kannata koskaan laittaa toimivassa muodossa www-sivulle, kirjoittaa vieraskirjaan, blogikeskusteluun tai lähettää verkkopostikortteja. Sähköpostiosoite tulee naamioida niin, ettei roskapostittaja löydä sitä julkisilta sivuilta. Tämä onnistuu esittämällä sähköpostiosoite kuvatiedostona, tai lisäämällä tekstimuodossa olevaan osoitteeseen ylimääräisiä merkkejä, jolloin osoitteita keräävä ohjelma ei osaa muuttaa niitä toimiviksi.

2. *Poista osoitteesi Internetistä.* Roskapostittajat löytävät Internetistä helposti uusia osoitteita listoilleen. Mikäli yritys tahtoo välttyä roskapostilta, kannattaa ehdottomasti poistaa tekstimuodossa olevat osoitteet Internet-sivustoilta. Osoitteen lopullinen poistuminen Internetistä saattaa kuitenkin viedä huomattavasti aikaa. Näin ollen osoitteiden laittamista tekstimuodossa Internetiin tulee lähtökohtaisesti välttää.

3. *Käytä piilokopioita.* On olemassa vakoiluohjelmia, joilla roskapostittajat keräävät sähköpostiosoitteita tarkoituksiinsa tavallisten käyttäjien koneilta. Mikäli organisaation sähköpostiosoite joutuu tällaisen henkilön haltuun, saattaa se joutua välittömästi roskapostittajan listalle. Lähetettäessä postia useille vastaanottajille, kannattaa käyttää kopiokentän (Cc) sijasta piilokopiokenttää (Bcc). Näin osoitteet eivät näy vastaanottajien koneilla, eivätkä sitä kautta päädy roskapostituslistoille.

4. *Varaa apuosoite webmailista.* Työpaikan sähköpostiosoitetta ei yleensä ole suositeltavaa käyttää henkilökohtaisen postin lähettämiseen tai vastaanottamiseen, eikä myöskään palveluihin jotka vaativat rekisteröityessä toimivan sähköpostiosoitteen. Niinpä onkin viisasta rohkaista työntekijöitä ottamaan käyttöön henkilökohtainen webmail-osoite, jota he voivat käyttää omaan viestintäänsä. Näin työntekijälle mahdollisesti tuleva roskaposti päättyy hänen henkilökohtaiseen webmail-osoitteeseensa, eikä näin haittaa organisaation verkkoliikennettä. Työntekijän sähköpostiahan ei ole luvallista yrityksen toimesta seurata, joten vastuu postin käyttämisestä luvallisiin tarkoituksiin jää työntekijälle. Tämän vuoksi on erittäin tärkeää että työntekijä ymmärtää vastuunsa sähköpostin käyttäjänä.



5. *Käytä suodatuspalvelua.* Yritys voi ostaa operaattoriltaan roskapostin suodatuspalvelun. Palvelu toimii esimerkiksi niin, että operaattori lisää epäilyyn roskapostiviestin otsikkoriville sanan [spam], jolloin loppukäyttäjän on helppo poistaa saapuneet roskapostiviestit. Monia erilaisia roskapostisuodattimia on olemassa, jotka palvelevat samaa tarkoitusta, vaikkakin hieman eri tavoin.

6. *Asenna roskapostin torjuntaohjelma.* Laajasti toimeksiantajan käytössä oleva F-Secure CS sisältää virustorjunta- ja palomuuriminäisyyksiensä lisäksi roskapostin torjuntaohjelman. Mikäli asiakas kaipaa suojaa roskapostilta, kannattaa ehdottomasti harkita jonkin torjuntaohjelman hankkimista. F-Securen hyvänä puolena voidaan pitää sitä, että samassa paketissa on kaikki tarpeellinen työaseman suojaamiseen, joskin ohjelma vaatii tietenkin suhteellisen paljon resursseja työasemalta. Pelkästään roskapostin suodattukseen tarkoitettuja ohjelmia on myös olemassa ja varmasti sellaisen hankkiminen maksaa nykypäivänä itsensä takaisin. Voidaanhan jo päätellä kuinka paljon organisaation työntekijöiltä kuluu päivittäin työaika roskapostin poistamiseen postilaatikoistaan.

7. *Hyödynnä käsittelysääntöjä.* Käsittelysääntöjä voi käyttää hyödyksi roskapostin suodatuksessa. Esimerkiksi .cn- ja .jp – päätteisistä osoitteista tulevat sähköpostit voi huoletta siirtää roskapostin tai suodattaa roskapostiksi, ellei sitten pidä yhteyttä kiinalaisiin tai japanilaisiin kollegoihin. Viestissä käytettävä merkkijärjestelmä (charset) myös paljastaa usein roskapostin ja tietyt otsikkokentässä olevat sanat kuten vaikkapa surullisen kuuluisa ”viagra”-sana, merkitsee tässä tapauksessa todennäköisimmin roskapostia.

8. *Vaihda sähköpostiohjelmaa.* Sähköpostiohjelmaa valittaessa kannattaa harkita tarkkaan ottaako käyttöön Windowsin mukana tulevan Outlook Expressin. Vaikkakin se on laajalti käytetty ohjelma, se ei sisällä roskapostin torjuntaa, eivätkä sen käsittelysääntönsä ole täysin ajanmukaisia. Esimerkiksi Office-paketin mukana tuleva Outlook 2003 sisältää jo automaattisesti päivittyvän roskapostisuodattimen.

9. *Luota ääkkösiin.* Tämä on käyttökelpoinen sääntö luotaessa sääntöjä roskapostisuodattimeen, sillä Suomalaiset viestit sisältävät useimmiten ä ja ö kirjaimia. Näin ollen ne on helppo tunnistaa yleensä asiallisiksi viesteiksi. Tietenkään sääntö ei ole niin käyttökelpoinen mikäli käyttäjällä on paljon englanninkielistä kirjeenvaihtoa.

10. *Älä peruuta, äläkä tilaa mitään.* Useimmiten mainosviestin lopussa on linkki josta voi mahdollisesti tilata jonkin tuotteen tai

poistua postituslistalta. Tällaiseen linkkiin ei kuitenkaan koskaan kannata luottaa, sillä monesti sen kautta vain kerätään tietoa roskapostittajalle, eli roskapostin määrä todennäköisesti lisääntyy mikäli käyttäjä seuraa linkkiä. (Järvinen 2007: 40 - 41)

### 3.7.3 Salaustekniikoista

Sähköpostin salauksen on tarkoitus toteuttaa luottamuksellisuuden, eheyden ja todennuksen periaatteet. Luottamuksellisuus tarkoittaa tässä yhteydessä sitä, että vaikka viesti päätyisi väärälle vastaanottajalle, sisältö ei silti paljastu. Eheys tarkoittaa sitä, ettei viestiä voida muokata matkalla lähettäjältä vastaanottajalle ja näin ollen voidaan olla vakuuttuneita tiedon oikeellisuudesta. (Järvinen 2003: 256)

Näillä periaatteilla ei käytännössä ole merkitystä ellei todennusta tapahdu. Toisin sanoen todennuksen avulla voidaan olla varmoja lähettäjän ja vastaanottajan henkilöllisyydestä. Tämä voi tapahtua esimerkiksi varmenteita käyttämällä. (Järvinen 2003: 256)

Salaaminen on kuitenkin hankalaa, sillä avainten hallinta ja periaatteiden ymmärtäminen vaatii paneutumista aiheeseen. On olemassa myös kansallisia rajoituksia, jolloin jotkin maat ovat halunneet kieltää tehokkaiden salausmenetelmien käytön ja näin ollen säilyttäneet mahdollisuuden kansalaistensa seuraamiseen, tai pyrkineet estämään salauksen leviämistä vihamielisiin maihin. Näistä poliittisista ongelmista johtuen ei ole syntynyt standardia joilla salaukset toimisivat eri ohjelmien välillä. Käytännössä suurin ongelma on lopulta se, että lähettäjä ja vastaanottaja joutuvat sopimaan etukäteen yhteisistä avaimista, tämä taas käy helposti työlläksi. Ongelma ratkeaa varmenteilla ja PKI-järjestelmällä (Public Key Infrastructure). Kaikille käyttäjille luotettavan ja tarpeeksi monen ihmisen tiedot kattavan PKI:n luominen on kuitenkin vaikeaa. (Järvinen 2003: 255 - 256)

Aivan ensimmäiseksi on syytä esittää kysymys, kuinka välttämätöntä on sähköpostin salaaminen? Voidaanko luottamuksellinen liikenne hoitaa jollain muulla tavoin? Onko tarve satunnaista vai jatkuvaa? On otettava huomioon, että esimerkiksi henkilötietojen ja tilinumeroiden lähettäminen sähköpostitse on arveluttavaa. Mutta mikäli se on yritykselle välttämätöntä, on ehdottomasti mietittävä keinoja sähköpostiliikenteen salaamiseen.

Vaihtoehtoja salattuun sähköpostiliikenteeseen ovat esimerkiksi tiedostoliikenteen salaaminen, salattu webmail, sekä varmenne ja tavallinen sähköposti. Mikäli yrityksen toiminta vaatii todella tehokasta salausta, on ehdottomasti otettava harkintaan PGP (Pretty

Good Privacy), joka on ”kaikkien vakavasti otettavien salausohjelmien äiti”. (Järvinen 2003: 287)

Tiedostoliitteen salaaminen tarkoittaa käytännössä sitä, että liitteenä lähetettävä tiedosto esimerkiksi pakataan pakkausohjelmalla, kuten Winzip ja suojataan pakkauksen yhteydessä salasanalla. Toinen vaihtoehto on suojata esimerkiksi Word-dokumentti tallennuksen yhteydessä salasanalla. Salasana on varminta lähettää vastaanottajalle jotain toista kautta, kuten esimerkiksi tekstiviestinä. Tiedostoliitteen salaaminen on järkevää silloin, kun tarve salaukseen on satunnaista. (Järvinen 2003: 257)

Toinen satunnaiseen salaustarpeeseen tarkoitettu keino on salattu webmail. Internetissä on tarjolla useitakin webmail-palveluita, jotka tarjoavat salattua sähköpostiviestintää. Lähettäjä siis avaa itselleen webmail-palveluun sähköpostitilin jota käytetään salausta vaativien viestien lähettämiseen. Salatun webmailin hyvä puoli on riippumattomuus paikasta. Sähköpostia voi siis lukea ja lähettää missä tahansa, missä on tietokone ja Internet -selain. Toinen hyvä puoli on, että viestien lukemisesta ei jää jälkiä tietokoneelle. Selain ei nimittäin tallenna palvelimelta luettuja sähköpostiviestejä välimuistiinsa. Yksi esimerkki salatusta webmail-palvelusta on CertifiedMail ([www.certifiedmail.com](http://www.certifiedmail.com)). (Järvinen 2003: 259)

Varmenne on eräänlainen sähköinen todistus lähettäjän henkilöllisyydestä. Varmenteen voi hankkia esimerkiksi Internetin kautta Verisignilta ([www.verisign.com](http://www.verisign.com)). Varmenne otetaan käyttöön sähköpostiohjelmassa ja salattavat viestit allekirjoitetaan varmenteella. Viestin salaaminen edellyttää vastaanottajan varmenteen hakeamista, jonka saa haettua esimerkiksi vastaanotetusta allekirjoitetusta viestistä. Kun vastaanottajan ja lähettäjän varmenteet on saatu kuntoon, voidaan aloittaa salattujen viestien lähettäminen. On kuitenkin muistettava että salattua sähköpostia voidaan lähettää vain varmenteessa mainittuun osoitteeseen. (Järvinen 2003: 263 - 275)

Mainittu PGP on ehkä kaikista vakavimmin otettava viestinnän salausohjelma. Sen käyttöliittymä on graafinen ja helpohko hallita, mutta periaatteiden sisäistäminen vaatii opettelua. PGP:tä ei olekaan tarkoitettu aivan tavalliselle loppukäyttäjälle. (Järvinen 2003: 287 - 291)

Salausmenetelmää mietittäessä on hyvä pitää mielessä kuitenkin yksi salaukseen liittyvä lainalaisuus, ”Kaikki salaukset ovat murrettavissa. Kyse on vain siitä, paljonko tarvitaan aikaa ja tietokone-tehoa”. (Järvinen 2003: 79)

### 3.8 Käyttäjätilit

Tietoturvallisuuden yksi peruspilareista on käyttäjän tunnistus. Jokaiselle käyttäjälle luodaan henkilökohtainen käyttäjätunnus, joka mahdollistaa käyttäjän tunnistuksen työasemaan kirjaututtaessa. Tunnistus varmistetaan sitä valvovassa järjestelmässä, jolloin väärä tai epäonnistunut kirjautumisyritys hylätään ja työaseman käyttö estyy. (Hakala ym. 2006: 124)

Jokaiselle käyttäjälle annetaan käyttäjätunnuksen kautta tietyt käyttöoikeudet. Pääsääntönä on, että jokaiselle käyttäjälle luodaan sellaiset oikeudet joilla työskentely on sujuvaa. Liian mittavat käyttöoikeudet lisäävät väärinkäytön riskiä mahdollistamalla käyttäjälle tuntemattomien ja väärin käytettynä työasemalle tai tietojärjestelmälle vaarallisten palveluiden käytön. Liian suppeat käyttöoikeudet puolestaan saattavat estää käyttäjälle tarpeellisten palveluiden käytön, jolloin työskentely ei onnistu tai viivästyy. Windows-järjestelmän peruskäyttäjäoikeudet riittävät yleensä työaseman sovellusten käyttöön. Järjestelmän pääkäyttäjäoikeudet puolestaan sallivat kaikkien palveluiden käytön, joten niiden käyttö tulee ehdottomasti rajata ainoastaan järjestelmänvalvojille. (Hakala ym. 2006: 128)

Käyttäjätilejä voidaan liittää tarpeen mukaan erilaisiin ryhmiin, jotka niin ikään mahdollistavat erilaiset oikeusmäärittelyt. Tämä helpottaa käyttäjien hallinnointia siten, että jokaiselle käyttäjälle ei tarvitse määritellä oikeuksia yksitellen. Käyttäjätili voidaan siis liittää ryhmään, jossa kaikki käyttäjät saavat samat käyttöoikeudet. (Hakala ym. 2006: 126 - 127)

Turvallisin tapa määritellä käyttöoikeuksia on antaa käyttäjälle ensin peruskäyttöoikeudet ja tarpeen mukaan lisätä käyttöoikeuksia. Näin estetään tehokkaimmin mahdolliset väärinkäytökset, jotka voivat olla tahattomia tai tahallisia. (Hakala ym. 2006: 126)

Koska tässä opinnäytetyössä on kyseessä ulkoistettu tietohallinto, tulee käyttäjäoikeuksien määrittelyn olla alusta saakka mahdollisimman tarkkaa. Jatkuva käyttäjäoikeuksien muokkaaminen saattaa kuluttaa huomattavasti toimeksiantajan resursseja. Onkin viisasta heti aluksi määritellä tarkasti käyttäjäryhmien sekä yksittäisten käyttäjien toimenkuvat ja tarvittut ohjelmistot, jolloin käyttöoikeudet voidaan räätälöidä alusta saakka sopiviksi. Kun asennusvaiheessa voidaan jo määritellä käyttäjän tarvitsemat ohjelmistot, voidaan käyttäjältä kieltää jatkossa ohjelmistojen asentaminen. Näin yrityksen työntekijät eivät voi tahallisesti tai tahattomasti asentaa yrityksen toiminnalle haitallisia ohjelmistoja työasemiinsa. Luvattomien tai lisensoimattomien ohjelmistojen käyttöön saattaa johtaa rikosoikeudellisiin seuraamuksiin. Mahdollisuuksien mu-

kaan kannattaa ottaa myös huomioon käyttäjien tietoteknisessä osaamisessa olevat puutteet. Tällöin käyttöoikeuksia ei parhaassa tapauksessa tarvitse muokata kuin vasta mahdollisten uusien ohjelmistojen käyttöönoton yhteydessä. (Miettinen 1999: 188)

Tärkeää on myös tässä yhteydessä pitää huolta siitä, että kun käyttäjä syystä tai toisesta poistuu lopullisesti organisaatiosta, myös käyttäjätunnus poistetaan. Esimerkiksi työsopimuksen päättyessä erimielisyyksiin tai riitaan, käyttäjä saattaa pystyä hyväksikäyttämään vielä käytössä olevaa tunnustaan ja poistamaan tai vahingoittamaan organisaation tietojärjestelmän sisältämiä tietoja.

### **3.9 Salasanat**

Salasana ja käyttäjätunnus on yleisesti tärkein suojausmenetelmä tietojärjestelmissä. Tämän vuoksi organisaation on huolehdittava siitä, että henkilöstö pitää huolta omista käyttäjätunnuksistaan ja salasanoistaan. Näin estetään niiden päätyminen väärin käsiin ja sitä kautta organisaation tietojärjestelmän luvaton käyttö. (Miettinen 1999: 235)

Salasanojen suojaamisessa tärkeimmät asiat ovat, että ne pidetään vain henkilökohtaisena tietona, niitä vaihdetaan tarpeeksi usein ja että ne ovat vaikeasti arvattavia. Viisainta on tietoturvallisuuskoulutuksen yhteydessä tai uuden työntekijän aloittaessa antaa myös ohjeistus salasanojen käytöstä. Ylläpitäjäkin voi vaikuttaa salasanojen muotoon käyttäjätilejä hallinnoimalla. Salasanoille voidaan esimerkiksi luoda vaatimuksia että niiden tulee sisältää vaikkapa yleisesti käytössä oleva kahdeksan merkkiä, tai että niiden tulee koostua isoista ja pienistä kirjaimista sekä numeroista ja erikoismerkeistä. Lisäksi voidaan määritellä kuinka usein järjestelmä pyytää käyttäjää vaihtamaan salasanan. Yleisesti salasanan vaihtoväliksi suositellaan kolmea kuukautta. Yleistä on myös, että käyttäjän kirjautuessa järjestelmään ensimmäisen kerran, järjestelmä pakottaa käyttäjän vaihtamaan oletussalasanansa. Nämä säännöt ovat erittäin yleisessä käytössä ja niitä on myös viisasta käyttää asiakasorganisaatioissa. Sääntöjen luonnin lisäksi on myös hyvä ohjeistaa työntekijää henkilökohtaisesti varmistamaan salasanan pysyminen vain työntekijän omana tietona. Käyttäjään ei tässä tapauksessa voida teknisesti valvoa, joten hänen omaa vastuutaan tulee korostaa. Käyttäjän tulee huolehtia mm. siitä, ettei kukaan näe kun hän kirjoittaa salasanan. Mikäli käyttäjä epäilee salasanan joutuneen ulkopuolisen tietoon, se tulee vaihtaa välittömästi. Salasanan kirjoittamista paperille tai tietojärjestelmän muistiin tulee välttää. Lisäksi kirjaututtaessa esimerkiksi toisen käyttäjän työasemalta omilla tunnuksilla, tulee varmistaa ettei työasema tallenna kirjautumistietoja muistiin. (Miettinen 1999: 236)

## 4 Fyysinen turvallisuus

Tässä kappaleessa käsitellään organisaation tietojärjestelmien fyysistä turvallisuutta kokonaisuudessaan ja pyritään ottamaan huomioon kaikki fyysiset uhkakuvat, joilta organisaation on toimialasta riippumatta syytä suojautua.

Fyysisellä turvallisuudella tarkoitetaan organisaation toimitilojen turvallisuutta tietojärjestelmien kannalta, sekä laitteistojen turvaamista fyysisiltä vahingoilta. Toimitilojen turvaamiseen kuuluvia osa-alueita ovat kulunvalvonta, murto-, sähkö-, palo- ja vesivahinkoihin varautuminen. (Hakala ym. 2006: 11 - 12)

Lisäksi käsitellään varmuuskopioiden, asennusmedioiden ja lisenssien turvaamista fyysisiltä uhilta. Laitteistojen turvaamiseen kuuluvat osa-alueet ovat laitteistojen fyysinen lukitus, turvamerkinnät, sekä laitteistojen ja komponenttien oikeaoppinen hävittäminen.

Fyysisen turvallisuuden valvominen on toimeksiantajan tapauksessa hieman kyseenalainen asia. Vaikkakin työasemien ja palvelinten fyysinen sijainti ja tila vaikuttaa tietoturvallisuuden toteutumiseen merkittävästi, kuitenkin ulkoistetulla yrityksellä ei ole suoranaista oikeutta puuttua asiakasorganisaation tilaratkaisuihin tai fyysiseen suojaukseen. Ainoa mahdollisuus on pyrkiä huomauttamaan asiakasyrityksen epäkohdista ja yrittää sitä kautta päästä ratkaisuun tietoturvallisuuden toteuttamisesta. Fyysinen turvallisuus on kuitenkin perustavanlaatuisen asia yrityksen tietojärjestelmien turvaamisessa, joten sitä ei voi missään tapauksessa kokonaan sivuuttaa.

Mikäli organisaatio tahtoo varmistua toimitilojensa turvallisuudesta, kannattaa kääntyä palo- ja pelastusviranomaisten, sekä rakennus-, vakuutus- ja turva-alojen konsulttien puoleen. He auttavat tietojärjestelmätilojen suunnittelussa ja näin yrityksen fyysinen turvallisuus saadaan perusteellisesti kuntoon. (Hakala ym. 2006: 305)

### 4.1 Kulunvalvonta

On tärkeää rajoittaa ja valvoa henkilöstön kulkemista kiinteistössä niin, että vain oikeutetut henkilöt pääsevät tiloihin joihin heidät on oikeutettu. Organisaation kiinteistössä täytyy muistaa ettei jokaisella työntekijällä ole pääsyä joka paikkaan. Esimerkiksi palvelin-tilat on lukittava niin, että vain ylläpitäjillä ja mahdollisesti joillakin tietyillä varmuuskopioinnista vastaavilla henkilöillä on oikeus ja mahdollisuus päästä tiloihin. Kulunvalvonnan arvo kasvaa sitä mukaa, mitä enemmän työntekijöitä yrityksessä työskentelee. (Miettinen 1999: 179)

Sähköinen lukitus mahdollistaa joustavan kulkuoikeuksien määrittelyn, joskin se on luonnollisesti kalliimpi toteuttaa kuin mekaaninen lukitus. Jos mekaaninen avain varastetaan, on edessä väistämättä lukkojen vaihto. Mikäli käytössä on sähköinen avainkortti, se voidaan ohjelmallisesti poistaa käytöstä järjestelmässä. Etenkin kun kyseessä on pieni tai keskisuuri yritys, kannattaa ehdottomasti miettiä miten lukitus saadaan hoidettua kustannustehokkaasti. (Miettinen 1999: 180)

#### *4.2 Murtovahinkojen torjunta*

Murtosuojauksen perusta on mekaaninen lukitus. Usein sen rinnalla käytetään erilaisia sähköisiä murtohälytysjärjestelmiä, tai sähköistä lukitusta. Kustannustehokkuus on usein tässäkin tapauksessa määräävä tekijä mitä pienemmästä yrityksestä on kyse. Luonnollisesti yrityksen kiinteän omaisuuden kasvaessa kasvaa myös tarve omaisuuden suojaamiselle. Murtosuojauksen toteutus on asiakasyrityksen harkinnan varassa, mutta tietojärjestelmän ylläpitäjän on tarpeen vaatiessa syytä puuttua puutteelliseen toteutukseen mikäli se merkittävästi alentaa muiden tietoturvaratkaisujen hyödyllisyyttä. (Miettinen 1999: 182)

Videovalvonta on hälyttimien rinnalla erittäin turvallinen järjestelmä, mutta kustannukset nousevat helposti korkeiksi. Mikäli yritys kuitenkin käyttää videovalvontaa, on viisasta asentaa myös palvelintiloihin videokamera. Varkauksien kannalta videovalvonta toimii ensinnäkin vahvana pelotteena ja toiseksi, se tallentaa mahdollisen tunkeilijan ajasta riippumatta ja auttaa näin mahdollisen rikoksen selvittelyssä. Videovalvonnan hankintaa suunniteltaessa kannattaa kuitenkin muistaa valita videomateriaalin tallennuspaikka huolella ja suorittaa kameran ja tallennuspaikan välinen kaapelointi harkitusti, eli ei mielellään pintakaapelointina. Usein käytetty tekniikka on tallentaa videokuvaa suoraan tietokoneen kiintolevylle. (Miettinen 1999: 180 - 182.) Viisas varas saattaa huomata kameravalvonnan, tai tietää siitä entuudestaan. Näin ollen kamerasta lähtevää kaapelointia seuraamalla varas löytää helposti kuvaa tallentavan tietokoneen ja vie mukanaan myös sen, jolloin videokuvaa ei tilanteesta ole enää saatavilla. Tämä episodi kannattaa siis pitää mielessä jos videovalvonta on ajankohtainen, sillä se perustuu todelliseen tapahtumaan.

Muutenkin organisaation sisäinen kaapelointi tulee toteuttaa huolella. Huolimattomasti sijoitetut, tai keskeisillä paikoilla jaloissa pyörivät kaapelit ovat jatkuvassa vaarassa niin tahallisten kuin tahattomienkin haittatekijöiden alaisena. Esimerkiksi ohi kulkeva henkilö saattaa vahingossa potkaista kaapelia joko irrottaen sen tai pahimmassa tapauksessa katkaisten koko kaapelin. Esimerkkinä vaikkapa Cat 6 (Category 6) kaapeli on erityisen herkkä rikkoutu-

maan päälle astuttaessa. Mahdollista on myös että vaikkapa juuri irtisanottu työntekijä tai edellisestä kappaleesta tuttu murtovaras tahtoo tahallaan tehdä organisaation toiminnalle kiusaa ja katkaisee sopivassa paikassa vastaan tulevan kaapelin aiheuttaen tietojärjestelmälle ongelmia. Kaapelointi on lisäksi sellainen järjestelmän osa, johon yleensäkin melko sokeasti luotetaan, eikä kaapeleita usein tutkita ensimmäisenä vian ilmetessä. Näin vika saattaa kummitella pitkäänkin verkossa aiheuttaen päänvaivaa organisaation tietojärjestelmävastaaville. Suositeltavinta onkin mahdollisuuksien mukaan piilottaa tietojärjestelmän kaapelointi toimitilojen rakenteisiin, tai suojata kaapelointia varten tarkoitetuilla kaapelointikouruilla (Miettinen 1999: 209).

Kaapelointiin liittyy edellisten lisäksi vielä yksi huomioon otettava seikka, tuhoeläimet. Kaapeloinnissa erityisesti jyrsijöitä houkuttelee verkko- ja telekaapeleiden notkisteaineena käytettävä rasva. Joten mikäli organisaation toimitiloissa on tavattu aikaisemmin jyrsijöitä, kannattaa se ottaa huomioon kaapeloinnin suunnittelussa ja selvittää sopivat torjuntakeinot. Myös muurahaiset ovat kiinnostuneita ATK-laitteista. Hyvin jäähdytetyissä palvelinhuoneissa ne saattavat hakeutua lämpimiin ATK-laitteisiin aiheuttaen niissä toimintahäiriöitä. Mikäli siis tietojärjestelmässä alkaa ilmetä mystisiä ja jatkuvia toimintahäiriöitä joille ei löydetä teknistä tai inhimillistä selitystä, saattaa todellinen vika löytyä palvelintilojen pieneläinmurtosuojauksesta. (Hakala ym. 2006: 306 - 307)

### ***4.3 Sähkövahinkoihin varautuminen***

Sähkövahinkoihin varautumiseen kuuluu olennaisimpana asiana erityisesti palvelinten ja muiden verkon ydinlaitteiden katkeamaton sähkönsyöttö, joka varmistetaan UPS-laitteella (Uninterruptible Power Supply). Ukkonen on yksi huomioon otettava seikka, joka saattaa aiheuttaa tietojärjestelmälaitteiden häiriöitä tai rikkoutumisia. Kuitenkin ukkosenjohdattimet kuuluvat kiinteistön omistajan vastuulle, joten niihin ei paneuduta tässä sen enempää. Lisäksi UPS antaa suojaa ukkosenkin aiheuttamilta sähkökatkoilta tai virtapiikeiltä. ISO 17799 –standardi edellyttää että rakennuksen sähkö- ja telenousujohdot on varustettu ylijännitesuotimilla. Mikäli näin ei kuitenkaan ole, asiakasyritykselle voi vain antaa suosituksia oikeasta toteutustavasta.

UPS-laitteen tarkoituksena on taata yrityksen tärkeimmille laitteille katkeamaton virransyöttö, niin että virta ehtii palaamaan järjestelmään tai laitteet ehditään sammuttaa turvallisesti sähkönsyöttöä kohdanneen katkon sattuessa. UPS-laitteiston tehtävä on myös suorittaa hallittu alasajo ennen kuin akut ehtyvät. (Hakala ym. 2006: 311)



Nykyaikainen ja myös toimeksiantajalla laajalti käytössä oleva UPS-laitteisto toimii niin, että se kytketään palvelimeen tai työasemaan, johon asennetaan päävalvontaohjelmisto (controller). Virran katkettua se antaa ilmoituksen virran katkeamisesta suojattaviin laitteisiin asennetuille valvontaohjelmistoille (member). Päävalvontaohjelmiston asetuksiin on määritelty kuinka kauan laitteet saavat toimia ennen niiden sammutusrutiinin aloittamista. Sähkövirran palatessa ennen sammutusrutiinin aloittamista UPS palauttaa sähkönsyötön ennalleen. (Hakala ym. 2006: 311 - 312)

Voimakkaat sähkömagneettiset- ja mikroaaltopulssit ovat myös yksi mahdollinen tietojärjestelmää kohtaava katastrofi. Voimakas sähkömagneettinen pulssi, eli EMP (Electro Magnetic Pulse) voi syntyä ydinräjähdysten tapahduttua ilmakehässä, jolloin sähkömagneettinen pulssi voi kulkea tuhansia kilometrejä pitkin ilmakehää. Pulssi kehittää tietojärjestelmälaitteiden virtapiireihin voimakkaan virran, joka polttaa piirit käyttökelvottomiksi tai ainakin häiritsee niitä vakavasti. Suurvaltojen kehittämät mikroaaltoaseet ovat puolestaan voimakkaiden mikroaaltopulssien lähde, jotka lamauttavat tietojärjestelmän. Sähkömagneettisilta pulseilta voidaan suojautua käyttämällä erityistä EMP-suojaa, joka on käytännössä metallihäkki johon tietojärjestelmän laitteet sijoitetaan. Vastaavaa järjestelmää käytetään myös mikroaaltopulseilta suojautumiseen. (Miettinen 1999: 184 – 185.) Kyseiset katastrofit ovat kuitenkin jo maailmanhistoriallisesti niin merkittäviä ja absurdeja, että niihin varautuminen kuuluu ainakin nykyisessä maailmanpoliittisessa tilanteessa vain korkeintaan puolustusvoimille ja muille kansantaloudellisesti kriittisille tahoille äärimmäisen uhan vallitessa.

#### ***4.4 Palo- ja vesivahinkoihin varautuminen***

Paloturvallisuus on Suomessa jo rakennusteknisiltä vaatimuksiltaan erittäin korkeaa luokkaa. Palovaroittimet ovat pakollisia kaikissa kiinteistöissä, joten lähtökohdat ovat hyvät. Erilaisia automaattisia paloilmoitinjärjestelmiä on paljon käytössä monissa organisaatioissa ja ne takaavatkin toiminnallaan nopean sammutusavun palon sattuessa. Automaattiset sammutusjärjestelmät, eli sprinklerit ovat myös käyttökelpoinen vaihtoehto palon syttyttyä. Kuitenkin niiden kanssa tulee olla tarkkana kun on kyse tietojärjestelmälaitteista. Sprinklerijärjestelmä ei ole suositeltava esimerkiksi palvelintilassa, koska vesi tekee yhtä suurta tuhoa laitteille kuin tuli, jolloin hyötysuhde on negatiivinen. Kun kyseessä on tila jossa käytetään paljon teknistä laitteistoa, oikosulun vaara luonnollisesti kasvaa. Onkin viisasta varata ensisammutusvälineet palvelintilan lähistölle. Vaahtosammuttimen sijasta kuitenkin sammutuspeite on mahdollisen palon syttyessä paras vaihtoehto. (Miettinen 1999: 183 – 184.) Paloturvallisuuteen liittyvät ratkaisut ovat kuitenkin lähinnä asiakasyrityksen vastuulla, mutta tässäkin tapauksessa

puutteellisesta turvallisuudesta on syytä huomauttaa mikäli aihetta on.

Helppoin tapa välttää tietojärjestelmään kohdistuvat vesivahingot, on järjestää tietojärjestelmälaitteille tilat joita ei ole viemäröity ja jotka eivät sijaitse tiloissa joissa on muuten välitön tulvaveden tai vuodoista johtuvan veden uhka. Palvelin- ja konehuoneisiin suositellaan 40-60%:n ilmankosteutta. Tämä voidaan toteuttaa ilmankostuttimella. Jos ilmankostutin on käytössä, tulee huomioida miten laitteen rikkoutumisesta johtuva tulvavesi saadaan johdettua pois tiloista. Sama koskee myös jäähdytysjärjestelmiä, joita usein käytetään palvelinhuoneissa. Lattiakaivot, sulkuventtiilit tai vuotoaltaat ovat hyviä ratkaisuja, mutta ne on myös pidettävä kunnossa. Vuosittaiset huoltokustannukset ovat joka tapauksessa pienemmät kuin järjestelmän korjauskustannukset vahingon sattuessa. (Hakala ym. 2006: 305)

#### ***4.5 Varmuuskopiot, asennusmediat ja lisenssit***

Tässä luvussa käsitellään organisaatiolle kriittisen materiaalin, kuten erityisesti varmuuskopioiden, asennusmedioiden ja lisenssien turvallista säilytystä.

Kenties alkeellisin virhe mitä varmuuskopioinnissa voi tehdä, on varmuuskopioiden säilyttäminen samassa paikassa, tai tilassa alkuperäisten tietojen kanssa. Esimerkiksi palo- tai vesivahingon sattuessa varmuuskopiot tuskin säästyvät alkuperäisiä tietoja paremmin. Murtovahingon sattuessa varas todennäköisesti saa käsiinsä niin alkuperäisen, kuin varmistetunkin datan. Viisainta onkin näin ollen säilyttää varmuuskopiot lukitussa, fyysisiltä uhilta suojatussa paikassa ja mielellään eri tilassa, tai jopa eri rakennuksessa kuin alkuperäinen data. (Miettinen 1999: 240)

Asennusmedioiden ja lisenssien säilyttämisessä on myös otettava huomioon että vain valtuutetut käyttäjät pääsevät niihin käsiksi. Esimerkiksi Microsoft Windowsin ja -Officen asennusmediat ovat varmasti haluttua tavaraa niin kotikäyttäjien, kuin varsinaisten rikkollistenkin keskuudessa. Tietämätön työntekijä ei välttämättä edes ymmärrä että on laitonta asentaa kotikoneelle työpaikalta ”lainattu” käyttöjärjestelmä tai ohjelmisto. Vielä suuremman uhan muodostavat ulkopuoliset, jotka saattavat tarkoituksellisesti etsiä ohjelmistojen tai käyttöjärjestelmien asennusmedioita ja niihin kuuluvia lisenssejä. Tämän vuoksi asennusmedioiden ja lisenssien säilyttämisestä tulee huolehtia samaan tapaan kuin varmuuskopioiden ja muun tärkeän aineiston säilyttämisestä.

Tässä tapauksessa tulee ottaa myös huomioon se, että toimeksiantaja saattaa tarvita mahdollisessa vikatilanteessa pikaisesti käsiinsä

alkuperäisen asennusmedian ja lisenssiavaimen jolla kyseinen ohjelmisto tai käyttöjärjestelmä asennetaan. Jos asennusmedia tai lisenssi on väärissä käsissä, sitä ei välttämättä koskaan löydy. Jos taas arkistointi on suoritettu huolimattomasti, saattaa kaivatun materiaalin etsintään kulua turhauttavan pitkä aika.

Suosittelavin vaihtoehto varmuuskopioiden, asennusmedioiden ja lisenssien säilyttämiseen on ehdottomasti dataturvakaappi. Se suojaa aineistoa kaikilta fyysisiltä uhilta mikäli sen käyttöön oikeutetut henkilöt on valittu huolellisesti. Dataturvakaappi on erityisesti datamateriaalin säilytykseen suunniteltu ratkaisu, joka suojaa materiaalia tulen ja veden lisäksi korkeilta lämpötiloilta joille materiaali on erityisen herkkää. Ainoa negatiivinen tekijä dataturvakaappin hankinnassa on hinta. Pienempienkin kaappien hankintaan kuuluu satoja euroja, joten pienelle organisaatiolle ei ehkä ole mielekästä hankkia dataturvakaappia. (Dataturvakaapit 2007)

Toimeksiantajalla onkin käytössään turvakaappi joka on tarkoitettu datamateriaalin säilytykseen. Näin ollen asiakasyrityksen kannalta kustannustehokkain ja paljon käytetty ratkaisu on säilyttää asiakasyrityksen asennusmedioita, lisenssejä ja pitempään säilytettäviä varmuuskopioita toimeksiantajan tiloissa. Tällöin materiaali on myös ylläpitäjän saatavilla viipymättä, eikä pääse ulkopuolisten käsiin.

#### **4.6 Laitteistoturvallisuus**

Laitteistoturvallisuudella tarkoitetaan yrityksen tietojärjestelmä-laitteiden asianmukaista suojaamista. Laitteiden toimintavarmuuteen, toimintatarkoituksen mitoittamiseen ja toiminnan testaukseen keskitytään luonnollisesti siinä vaiheessa kun laitteita hankitaan tai kootaan. (Miettinen 1999: 21.) Huollon järjestäminen kuuluu myös laitteistoturvallisuuteen ja siitä huolehtii tässä tapauksessa toimeksiantaja. Toimeksiantaja on jo ylläpitosopimuksen mukaan velvollinen huolehtimaan asentamiensa laitteiden laadusta ja toimintavarmuudesta, joten tässä luvussa keskitytään lähinnä varkauksien estoon liittyviin fyysisiin suojausmenetelmiin. Lisäksi käsitellään laitteistojen ja komponenttien oikeaoppista hävittämistä.

##### **4.6.1 Laitteistojen fyysinen lukitus**

Tietojenkäsittely- ja tietoliikennelaitteiden fyysiseen lukitukseen on olemassa monenlaisia ratkaisuja. Laitteet on järkevää lukita varsinkin organisaation julkisissa tiloissa ja niissä tiloissa joissa yleensä asioi paljon ulkopuolisia. Fyysinen lukitus toimii varkautta ennaltaehkäisevänä ja hidastavana tekijänä. Jos laitteet on lukittu, varas saattaa jättää laitteiden irrottamisen sikseen. Mikäli käytetään automaattista hälytysjärjestelmää, lukitus saattaa hidastaa lait-

teiden irrottamista niin, että viranomaiset ehtivät paikalle ennen kuin varas saa laitteiden lukituksen purettua. (Miksi suojautua? 2007)

Paikallisten työasemien lukitukseen voidaan käyttää esimerkiksi ankkuri/vaijerilukitusta. Eli käytännössä työaseman näyttö ja keskusyksikkö lukitaan vaijerilla työpisteeseen. Lukitustelineellä voidaan lukita itse keskusyksikkö esimerkiksi työpöytänsä. On myös olemassa lukitusjärjestelmä, jolla estetään kotelon avaaminen ja johon voidaan haluttaessa kiinnittää myös näppäimistön ja hiiren johto varkauden estämiseksi. Kannettaville tietokoneille ja näytöille on olemassa erilaisia vaijerilukituksia, joilla tietokone tai näyttö lukitaan työpisteeseen. Lisäksi kannettavan tietokoneen tai vaikkapa videotykin voi kiinnittää työpisteeseen vaijerilla, johon on yhdistetty hälytys. Hälytys laukeaa jos vaijeri katkaistaan tai laitetta liikutellaan toistuvasti. CD/DVD-, levyke- ja Zip-aseman lukitus on myös mahdollista, jolloin estetään aseman luvaton käyttö. Näin ollen tietojen luvaton kopiointi ja virusten leviäminen levyasemien kautta on myöskin estetty. Näistä vaihtoehdoista on hyvä lähteä miettimään tilanteeseen sopivaa lukitusta. (Tuotteet... 2007)

Tässä tapauksessa fyysistä lukitusta suunniteltaessa on tärkeää muistaa että ylläpitäjä tarvitsee mahdollisessa vikatilanteessa viipymättä pääsyn laitteelle. Eli mikäli laitteita lukitaan, on huolehdittava että avain on jatkuvasti ylläpitäjän saatavilla.

#### 4.6.2 Turvamerkinnot

Laitteiden turvamerkintä toimii niin ikään varkauksia ennaltaehkäisevänä tekijänä, sillä turvamerkityn laitteen jälleenmyynti on huomattavasti hankalampaa kuin merkkeämättömän. Lisäksi mahdollisuus laitteen takaisin saamiseen on suurempi. Myös poliisi ja vakuutusyhtiöt suosittelevat laitteiden turvamerkintää. Etenkin kannettavien laitteiden turvamerkintä on viisasta, sillä ne ovat yleensä organisaation laitteista eniten alttiina ulkopuolisille henkilöille ollessaan organisaation ulkopuolella. Tamperelainen Innosec Oy tarjoaa kahta erilaista turvamerkintätapaa - ID2S ja EuroMark. (Miksi suojautua? 2007)

ID2S-turvamerkintä toteutetaan asentamalla merkittävään laitteeseen turvamerkintälaatta, joka sisältää yksilöllisen tunnistenumeron ja tiedot laitteen omistajatietojen tarkastamista varten. Laatan irrottamiseksi vaaditaan 400 kg:n voima. Laatan alla on vielä varmistelaatta joka sisältää samat tiedot kuin varsinainen turvamerkintälaatta. Varmistelaatta vulkanoituu laitteeseen, eli jos laatta saadaan poistettua, ovat tunnistetiedot edelleen luettavissa. Yksilöllisen numerosarjan tunnistetiedot on tallennettu maailmanlaajuisen tietokantaan. Laitteen kadotessa se ilmoitetaan tietokannan

mustalle listalle. Viranomaisilla ympäri maailman on pääsy tietokantaan, jolloin laitteen löytyessä se voidaan tunnistaa tietojen perusteella ja palauttaa oikealle omistajalleen. (Turvamerkintä - ID2S 2007)

EuroMark-turvamerkintä suoritetaan etsaamalla organisaation haluat tunnistetiedot pintaa syvemmälle haluttuun laitteeseen. Turvamerkinnän poistaminen ilman näkyviä jälkiä on näin ollen mahdotonta. Molemmat turvamerkinnät voidaan suorittaa itse asiakasorganisaation tai toimeksiantajan toimesta. (Turvamerkintä - EuroMark 2007)

#### **4.6.3 Laitteistojen ja komponenttien oikeaoppinen hävittäminen**

Organisaation tarpeettomaksi käyneen tai vanhentuneen tiedon hävittäminen on tiedon elinkaaren viimeinen vaihe. Huolimaton tiedon hävittäminen saattaa johtaa organisaatiolle luottamuksellisen tiedon paljastumiseen ja sitä kautta ongelmiin lainsäädännön tai yhteistyökumppaneiden kanssa. Tiedon oikeaoppinen hävittäminen koskee tietenkin organisaation kaikkea tietoaineistoa. (Miettinen 1999: 191 – 192.) Kirjallisen tietoaineiston hävittäminen jää luonnollisesti asiakasorganisaation vastuulle joten tässä yhteydessä tietoaineiston hävittämisen kannalta keskitytään magneettisiin ja optisiin muistivälineisiin, kuten CD, DVD, varmistuksessa usein käytettävät magneettinauhat, levykkeet ja kiintolevyt. Näiden hävittämiseen on toimeksiantajalla selkeät tiedon hävittämiserutiinit.

Magneettisille ja optisille muistivälineille tallennetut tiedot voidaan hävittää mekaanisesti silppuamalla ne pieniksi palasiksi. Näin usein toimitaankin kun on kyseessä esimerkiksi rikkoutunut kiintolevy. Tätä menetelmää käyttämällä tietojen palauttaminen ei ole yleensä enää mahdollista, ainakaan ilman mittavia ponnisteluja, eikä muistivälinettä voida enää uudelleen käyttää. Mikäli muistiväline kuitenkin tahdotaan uudelleenkäyttöön, voidaan muistivälineen sisältämä tieto hävittää sähköisesti päällekirjoittamalla. Optisen muistivälineen, kuten CD tai DVD ollessa kyseessä tämä ei tietenkään ole mahdollista, ellei käytetä CD/DVD-RW (ReWritable) –levyjä. (Miettinen 1999: 193 - 194)

Kiintolevyn tietojen tuhoaminen sähköisesti on ehkä yleisin toimenpide organisaatioissa silloin, kun edellisen käyttäjän tiedot halutaan poistaa ja kiintolevy siirtää uudelle käyttäjälle. Täytyy kuitenkin muistaa että yksi päällekirjoituskerta ei riitä luotettavaan tiedon hävittämiseen. Yhdysvaltain puolustusvoimien päällekirjoitusstandardin (DOD 5220-22M) mukaan seitsemän päällekirjoituskertaa takaa luotettavan tietojen poistamisen. Luotettavaan tietojen poistoon on myös tehty apuohjelmia, joista Norman Ibas Oy:n kehittämä Expert Eraser on yksi vartenotettava vaihtoehto

joka myös noudattaa kyseistä standardia. Expert Eraser suorittaa tietojen poiston kiintolevyiltä niin, että ensimmäinen päällekirjoitus tehdään purkuvarmalla satunnaisjaksolla (ISAAC-algoritmi), seuraavat viisi nollilla ja ykkösillä ja viimeinen kaikkien lohkojen päällekirjoitus lohkon otsikolla ja täytemateriaalilla. Näin tiedot saadaan riittäväällä varmuudella hävitettyä ja kiintolevy voidaan ottaa jälleen käyttöön. (Expert Eraser... 2001)

Demagnetisointi on myös yksi tapa suorittaa magneettisten muistivälineiden sisältämän tiedon tuhoaminen niin, että ne voidaan uudelleen ottaa käyttöön. Muistivälineet asetetaan alttiiksi voimakkaalle magneettikentälle, jolloin kaikki tiedot häviävät muistivälineen magneettisuuden kadotessa. Menetelmä on kuitenkin hidas ja kallis, joten sen käyttäminen tuhoamismenetelmänä ei tule kyseeseen tässä tapauksessa. (Miettinen 1999: 193)

## 5 Tietoliikenneturvallisuus

Tietoliikenneturvallisuuden alla käsitellään lähes kaikki tietoliikenteen tekniseen suojaamiseen kuuluvat asiat. Olennaisia asioita tietoliikenteen turvaamiseen liittyen ovat tietoliikennejärjestelmän kokoonpano, dokumentointi, ylläpito, ongelmien kirjaus, sekä käytön- ja pääsyn valvonta. Pääsynvalvonnasta vastaa palomuuuri. Käytönvalvontaan kuuluvat lähinnä lokitietojen seurantaan ja keräämiseen liittyvät käytännöt, joka on itse asiassa yksi tärkeimmistä tietoliikenneturvallisuuden osa-alueista. Myös ohjelmistojen turvallisuus kuuluu tietoliikenneturvallisuuteen. (Rousku 2003: 54 - 56)

Näiden lisäksi tässä yhteydessä käsitellään myös tietoverkkojen olennaisimpia uhkatekijöitä, reititystä ja kytkimiä, palvelimia, virusturvaa, sekä tietoaineistoturvallisuutta. Tietoaineistoturvallisuutta pidetään käytännössä täysin omana osa-alueenaan tietoturvallisuutta määriteltäessä, mutta koska se on vahvasti sidoksissa varmuuskopiointiin, on se viisasta käsitellä tässä yhteydessä.

Koska tietojärjestelmän tekninen suojaaminen on sinällään todella laaja käsite, aivan kaikkea ei tässä yhteydessä pystytä yksityiskohtaisesti käsittelemään. Mahdollisimman suuri osa tietoturvallisuuteen liittyvistä seikoista on kuitenkin pyritty ottamaan huomioon ja löytämään niiden toteuttamiseksi yleiskäyttöiset ja toimeksiantajan käytäntöihin perustuvat ratkaisut.

### 5.1 Uhkatekijät tietoverkoissa

Virusten, haittaohjelmien ja muiden Internetin tuomien uhkien yksityiskohtainen tarkastelu tässä yhteydessä ei ole järkevää eikä edes käytännössä mahdollista. Näin ollen tässä yhteydessä pyritäänkin lähinnä antamaan yleiskuva tietoverkkojen uhkatekijöistä.

Virusten määrä kasvaa jatkuvasti huimaa vauhtia, samoin haittaohjelmien. Tästä kertoo jo F-Securen tietoturvyhteenveto heinä-joulukuulta 2005, jossa tunnettujen virusten määräksi kerrottiin jo 150 000 kappaletta. Samassa yhteydessä F-Secure kertoo American Language Centerin toimeenpanemasta roskapostikampanjasta, jonka seurauksena yli 20 miljoonaa venäläistä sähköpostiosoitetta sai roskapostia kyseiseltä taholta. Phishing-verkkohuijaustekniikka on yksi nykyajan kirouksista, jonka seurauksena saksalaiset pankit ovat ilmoittaneet menettäneensä 70 miljoonaa euroa vuoden 2004 aikana. Huijareiden keksintö hyödyntää URL-osoitteiden kirjoitusvirheitä on luonut mahdollisuuden tehdä uusia sivustoja, kuten ”google”, jotka vievät käyttäjän Google-hakukoneen sijasta haittaohjelmia sisältävälle sivulle. (F-Secure tietoturvyhteenveto... 2005)

F-Securen tietoturvakatsaus heinä-joulukuulta 2006 kertoo vielä uusimmasta trendistä, eli mobiililaitteiden haittaohjelmista. Niiden lukumäärä ylitti vuoden 2006 loppuun mennessä 330 kappaletta ja jatkuvasti löydetään uusia. (F-Secure tietoturvakatsaus... 2006)

Kehittyvistä tietoturvauhista kerrotaan myös MikroBitti-lehdessä syyskuulta 2006. Kyseessä ovat ns. kaapparitrojialaiset. Troijalainen siis kaappaa uhrinsa kiintolevyn ja salakirjoittaa sen. Kiintolevyn sisällön takaisin saaminen edellyttää vaaditun summan maksamista ohjelman tekijälle. Troijalainen on käyttänyt aikaisemmin 56-bittistä salausta, joka on vielä suhteellisen helppo avata. Nykyään kyseinen Gpcode-trojialainen on siirtynyt kuitenkin käyttämään jo 660-bittistä RSA-salausta. Kyseisen salauksen purkamiseen menisi Kaspersky-yhtiön laskelmien mukaan 2,2 gigahertsin tietokoneelta 30 vuotta. Kasperskyn mukaan on vain ajan kysymys milloin troijalaisissa aletaan käyttää vieläkin järeämpää salausta. (Supertrojialaiset... 2006: 10)

On myös olemassa erilaisia sähköposti-, verkko- ja bluetooth-matoja, jotka hyödyntävät ohjelmistojen ja järjestelmien heikkouksia päästäkseen sisään tietojärjestelmään. Näihin eivät auta perinteiset virustorjuntaohjelmat. Ainoa tekninen suojautumiskeinomattoja vastaan on palomuurijärjestelmä. Madot voivat esimerkiksi kerätä tietoa järjestelmästä ja lähettää sitä verkon yli epäluotettavalle taholle. Toinen vaihtoehto on, että mato aiheuttaa muita hädästäviä tai haitallisia vaikutuksia tietojärjestelmässä. Samaan tapaan toimivat ns. Troijan hevoset ja spyware-ohjelmat (vakoiluohjelmat). Spyware-ohjelmien ja virusten keskeinen eroavaisuus on, että virukset leviävät nopeammin, sillä spyware-ohjelma tarvitsee yleensä asentaa käyttäjän toimesta, virus puolestaan toimii automaattisesti. (F-Secure jälleenmyyjäkoulutus 2006: 28 - 32)

Toisenlaisen uhan muodostavat hyökkäykset, jotka tapahtuvat ihmisten toimesta. Yksi uhka on esimerkiksi DoS-hyökkäys (Denial of Service). Hyökkääjä voi tässä tapauksessa esimerkiksi lähettää valtavan määrän sähköpostiviestejä lyhyen ajan sisällä sitoakseen organisaation sähköpostipalvelimen kaikki resurssit ja näin lamauttaakseen sen toiminnan. (F-Secure jälleenmyyjäkoulutus 2006: 34)

Man-in-the-middle -hyökkäys on myös hyvä esimerkki. Tässä tapauksessa hyökkääjä kaappaa lähettävältä taholta tulevan DNS-palvelimelle (Domain Name System) suunnatun nimikyselyn, johon hän vastaa lähettämällä oman IP-osoitteensa. Näin liikenne lähettävältä taholta kulkee oikean DNS-palvelimen sijasta hyökkääjän tietokoneen kautta. Tämä mahdollistaa viestien salakuuntelun tai manipuloinnin. Erityisen vaarallinen tilanne on, jos hyökkääjä



onnistuu saamaan käsiinsä luottamuksellista tietoa, tai kykenee manipuloimaan sitä. Ainoa tapa man-in-the-middle -hyökkäyksen estämiseksi on lähettäjän ja vastaanottajan todennus. Tämä onnistuu esimerkiksi varmenteita käyttämällä. (Järvinen 2003: 120 - 121)

Edellä mainitut Internetin tuomat uhat ovat vain pieni pala tietojärjestelmiä koskettavista uhista ja lähes päivittäin löydetään uusia. Näin ollen ei liene epäselvää minkä vuoksi virustorjunnan ja palomuurin käyttöä sekä päivityksistä huolehtimista korostetaan tietojärjestelmissä.

## **5.2 Dokumentointi**

Riittävä dokumentointi on tietoturvallisuuden edellytys. Se helpottaa teknistä ylläpitoa, tietojenkäsittelyä ja tietohallintoa. (Hakala ym. 2006: 32)

Hyvä lähtökohta verkon dokumentoinnille on verkon kuva, joka sisältää tietojärjestelmälaitteet yksilöivine tietoineen. Hyvä nyrkkisääntö onkin: ”jos et pysty piirtämään sitä, et pysty rakentamaan sitä”. (Allen 2002: 127)

Organisaation laitteiston dokumentointi on myös erittäin tärkeää ja mm. vakuutusyhtiöt saattavat dokumenttia organisaation kaikista laitteista.

Palomuurin suodatussäännöt on niin ikään viisasta dokumentoida ja varustaa kukin sääntö selityksellä säännön tarkoituksesta. Näin jokainen joka lukee dokumentaation voi päätellä miten palomuri toteuttaa suodatuksen. (Allen 2002: 154)

Tietoturvapoliitikan toteutumisen edellytys on, että se jaetaan selkeästi ohjeiksi, toimenpiteiksi ja käytännöiksi. Käytännössä se tarkoittaa tarvittavan dokumentoinnin luomista henkilöstön käytettäväksi. Kattava dokumentaatio sisältää mm. tietoturvaan liittyvän lainsäädännön, riskianalyysin, yrityksen tietoturvaohjeistuksen, työntekijöiden tietoturvakoulutus-, jatkuvuus- ja toipumissuunnitelman, käyttöoikeuksien määrittelyn, järjestelmien käytön valvontasuunnitelman, käyttäjien, ylläpitäjän ja johdon vastuuden määrittelyn, sekä toimenpiteet väärinkäytöksissä ja tietoturvan loukkaustilanteissa. (Rousku 2003: 54 - 56)

Ymmärrettävästikin kaiken edellä mainitun dokumentointi ja ylläpitäminen ei onnistu pienemmältä yritykseltä jolla ei yksinkertaisesti ole henkilöstöresursseja dokumentoinnista huolehtimiseen. Myöskään ylläpitäjä ei pysty huolehtimaan kaikesta asiakasorganisaation dokumentoinnista, sillä työtä riittää organisaation tietojär-

jestelmän ylläpitämisessä muutenkin. Näin ollen pienemmässä asiakasorganisaatiossa dokumentoinnista on syytä poimia olennaimmat asiat, jotka ovat riskianalyysi, uhkiin varautuminen ja niiden torjunta, sekä käyttäjäohjeistukset. (Rousku 2003: 54 - 56)

Yleinen virhe dokumentoinnissa on ylläpito, tai jopa dokumentoinnin täydellinen laiminlyönti. Dokumentoinnista ei juurikaan ole hyötyä, mikäli sitä ei ole päivitetty esimerkiksi laitteiston muuttuessa. Puutteelliseen dokumentointiin liittyy usein organisaation vastuuhenkilöiden ajan puute, jolla ylläpidon laiminlyöntiä puolustellaan. Todellisuudessa dokumentoinnin päivittäminen jälkikäteen vie kuitenkin moninkertaisesti aikaa verrattuna dokumentoinnin jatkuvaan ylläpitoon. (Hakala ym. 2006: 32)

Olennaista on myös muistaa että dokumentit pidetään vain niiden käyttäjien saatavilla, jotka niitä todellisuudessa tarvitsevat. Mikäli dokumentit joutuvat potentiaalisen hyökkääjän haltuun, hyökkääjä saattaa pystyä käyttämään helposti hyväkseen dokumenteissa ilmeneviä tietoja.

### ***5.3 Järjestelmän- ja käytönvalvonta***

Yrityksen tietojärjestelmän ja laitteiden käytön valvonnalla on tarkoitus varmistaa käyttöoikeuksien noudattaminen ja selvittää tahalliset sekä tahattomat virhetilanteet. Käytännössä pyritään valvomaan, että vain oikeutetut käyttäjät käyttävät heille määriteltyjä resursseja. Lisäksi voidaan reaaliajassa tai jälkikäteen seurata vika-tilanteita, jotka voivat olla joko tahallisia tai tahattomia. Näin ongelmiin voidaan viipymättä reagoida niiden vaatimalla tavalla. Tärkein seurantamenetelmä on tietojärjestelmän lokitiedot. (Miettinen 1999: 237)

Lokitiedot ovat järjestelmän tapahtumatietoja, jotka tallentuvat tietojärjestelmälaitteen muistiin nykyaikana yleensä automaattisesti ja reaaliajassa. Esimerkkinä Windows XP –käyttöjärjestelmä, joka kerää reaaliajassa koneen tapahtumat lokitiedostoon. Lokitiedostoja pääsee selaamaan ohjauspaneelin alta, josta löytyvät valvontatyökalut. Niihin kuuluu tapahtumien valvonta, joka kerää sovellus-, suojaus- ja järjestelmä –lokitiedostoja. Sovellus-loki, kerää sovellusten toimintaan liittyviä tapahtumia. Suojaus-lokin tarkoitus on kerätä tietokoneen suojaukseen liittyviä tapahtumia. Järjestelmäloki kerää puolestaan tietokoneen fyysisen laitteiston aiheuttamia tapahtumia. Tapahtumat luokitellaan tärkeytensä mukaan virheiksi, varoituksiksi tai yleisiksi sovelluksen toimintaan liittyviksi tiedoiksi. Näistä luonnollisesti varoitukset ja virheet ovat niitä jotka aiheuttavat toimenpiteitä ja joita tulee seurata tarkasti.

Kaikkia tapahtumia ei missään tapauksessa ole tarkoitus seurata. Tavoitteena on seurata niitä tapahtumia joilla on todellisuudessa merkitystä organisaation turvallisuudelle. Olennaista on että saadaan tietää mitä on tapahtunut, milloin ja mistä se on aiheutunut. (Hakala ym. 2006: 101 - 102)

Käyttäjien valvonnassa edelliset ovat niin ikään oleellisia tietoja. Lisäksi on syytä tietää käyttäjätunnus joka on mahdollisia ongelmia aiheuttanut. Näin voidaan lähteä selvittämään ongelmaa tarkemmin ottamalla yhteyttä käyttäjään. (Miettinen 1999: 237)

Käyttäjien valvonnan rinnalla on myös tärkeää saada tietoa laitteiden fyysisestä toiminnasta, sekä sovellusten toiminnasta. Tärkeää on myös kyetä tunnistamaan kaapeloinnissa sattuneet vikatilanteet. Näin myös laitteiden ja ohjelmistojen rikkoutumiseen voidaan reagoida. (Hakala ym. 2006: 259)

Lokitiedostoja seurattaessa havaitut ongelmat on syytä dokumentoida huolellisesti. Olennaista ongelman dokumentoinnissa on sen tapahtuma-aika, ongelman kuvaus, laite jossa ongelma on havaittu, sekä sen ratkaisumenetelmä. Käytäntönä toimeksiantajalla on yksinkertainen excel-taulukko, johon on kirjattu asiakasorganisaation kaikki seurattavat laitteet. Taulukko sisältää erikseen mm. palvelimet, varmuuskopiointiohjelmistot ja virustorjuntaohjelmistot. Kuhunkin kategoriaan merkataan ongelma ja sen yksilöivät tiedot. Aiemmin tapahtuneiden ongelmien ratkaisumenetelmiä voidaan näin käyttää ohjeina niiden ilmestyessä uudelleen. Lisäksi voidaan seurata ongelmien ilmestymistiheyttä. Tällöin ongelmien uusiutuksessa voidaan harkita uutta ratkaisutapaa, joka poistaa ongelman kokonaisuudessaan. Dokumentoinnilla on myös tarkoitus helpottaa ylläpitäjän vaihtamista. Mikäli esimerkiksi ensisijainen ylläpitäjä on estynyt lokien tarkastuksesta, toinen ylläpitäjä voi suorittaa tarkastuksen helposti dokumentaatiota apuna käyttäen. Ensisijaisesti seurattavia lokeja ovat palvelinten sovellus- ja järjestelmälokit, joista poimitaan virheet ja varoitukset. Näihin etsitään sopivat ratkaisumetodit, jotka niin ikään kirjoitetaan dokumentaatioon.

ISO 1779 –standardi jakaa teknisen seurannan neljään pääkohtaan. Virhelokiin kerätään laitteisto- ja järjestelmävirheet. Operaattori- ja pääkäyttäjälokiin kerätään kyseisten käyttöoikeuksien haltijoiden tekemät toiminnot. Järjestelmien käytön seuranta -lokiin määritellään käytön valvonnan menettelytavat. Auditointilokiin kirjaetaan käyttäjien kirjautumistapahtumat, etenkin sallitusta poikkeavat. (Hakala ym. 2006: 102)

## 5.4 Reititys ja kytkimet

Reititys tarkoittaa prosessia, jossa päätetään miten reitittimelle tulevaa pakettia käsitellään. Käytännössä paketti joko päästetään läpi tai suodatetaan pois reitittimen suodatussääntöjen perusteella. Suodatussäännöt on konfiguroitu reitittimen reititystauluun, jota reititin käyttää suodatuspäätöstä tehdessään. (Allen 2002: 148)

Kuitenkin nykyään sisäverkoissa pyritään välttämään reitittimien käyttöä. Reititin on verkkokerroksen laite, joka toimii hitaammin kuin siirtoyhteyskerroksella toimivat aktiivilaitteet. Reitittimet joutuvat käsittelemään IP-otsakkeen ja tilanteen mukaan TCP- tai UDP-otsakkeen tietoja. Kytkin sen sijaan käsittelee yleensä vain ethernet-otsakkeen tietoja. Kytkimet huolehtivat nykyaikaisissa lähiverkoissa kuormantasauksesta, varayhteyksistä, liikenteen priorisoinnista ja käyttäjän tunnistukseen perustuvasta yhteyksien hallinnasta. Näin ollen myös vikasietoisten verkkojen toteuttaminen onnistuu kytkimillä. Välttämättä kytkin ei tarvitse minkäänlaista manuaalista konfigurointia, mutta useimpia kytkimiä päästään hallintaominaisuuden avulla muokkaamaan organisaation tarpeiden mukaan. (Hakala ym. 2006: 227)

Yrityksen sisäverkkoa luonnollisesti suojaa palomuuuri, jonka takana tietojärjestelmälaitteet ovat suhteellisen hyvässä turvassa. Näin ollen reitittimillä ja kytkimillä ehkä olennaisimmat tietoturvasuuteen liittyvät toimenpiteet liittyvätkin etähallintaan ja käyttäjän tunnistukseen. Mikäli ei ole täysin välttämätöntä, reitittimien ja kytkimien etähallinta tulisi kieltää. Käytännössä siis kielletään teknisesti hallintaominaisuuksiin pääsy ulkopuolelta. Lisäksi käyttäjän tunnistus on hoidettava huolellisesti. Tällöin vain asianomaisilla, eli käytännössä ylläpitäjällä on oikeus päästä käsiksi reitittimien hallintaominaisuuksiin.

Kolmantena toimenpiteenä tulee ehdottomasti mahdollisuuksien mukaan sulkea käyttämättömät portit. Tämä on hyvä keino estää vieraan tietojärjestelmälaitteen liittäminen fyysisesti lähiverkkoon.

Aiheen laajuuden vuoksi tässä yhteydessä ei reitittimiin ja kytkimiin voida tutustua perusteellisemmin, mutta näillä perustavanlaatuisilla toimenpiteillä ja tietenkin huolellisella konfiguroinnilla varmistetaan laitteiden tietoturvasuus.

## 5.5 Palvelimet

Palvelinten suojaamisessa ensimmäinen toimenpide on asentaa vain minimikonfiguraatio, eli ne palvelut, joita edellytetään verkon toiminnan takaamiseksi. Tämä tehdään mm. siitä syystä ettei palvelinta kuormiteta turhaan, jolloin tärkeimpien palvelujen ja näin

ollen koko verkon toiminta saatetaan uhanalaiseksi. Minimikonfiguraatiota käytettäessä ylimääräiset palvelut eivät myöskään aiheuta väärinkäytön uhkaa. Järjestelmää asennettaessa on lisäksi asennettava käyttöjärjestelmän sekä ohjelmistojen paikkaukset ja päivitykset viipymättä, sillä onnekas hyökkääjä saattaa osata hyödyntää järjestelmän aukkoja heti kun laite liitetään verkkoon. Palvelinten turvaamista mietittäessä on myös tärkeää ottaa huomioon palvelimelle tallennetun tiedon luottamuksellisuuden turvaaminen, eli että vain valtuutetut käyttäjät pääsevät käyttämään palveluita ja tietoja ja vain niitä palveluita joihin heillä on valtuutus. Palvelintila on siis syytä suojata asiattomalta pääsylvä ja etäkäyttö mahdollistaa vain järjestelmänvalvojien työasemilta salatulla yhteydellä ja mielellään käyttämällä vahvaa tunnistusta. Lisäksi komponenttien ja palvelinten kahdentaminen on aina järkevä keino haavoittuvuuksien, kuten datan häviämisen tai laitteistovikojen aiheuttamien riskien minimoimiseksi. (Hämäläinen 2007: 49 - 50)

Kahdentaminen luonnollisesti kasvattaa kustannuksia, mutta saattaa suuressa järjestelmässä olla erittäin viisas ratkaisu. RAID-kiintolevyt (Redundant Array of Independent Disks) ovat palvelimissa aina järkevä ratkaisu ja toimeksiantajalla yleinen käytäntö. Peilaus-tekniikalla (mirroring) kaksi tai useampia kiintolevyjä liitetään yhdeksi loogiseksi levyksi jolloin yhden fyysisen levyn hajoessa dataa ei menetetä, sillä se on tallennettu kahdelle tai useammalle erilliselle kiintolevyille. RAID-ratkaisu on verrattain halpa palvelimen vikasietoisuuden kasvattamiseksi. (Hakala ym. 2006: 140)

Edellisten lisäksi on tärkeää ylläpitää tietojen eheyttä, eli että tietoja ei tuhoudu tai korruptoidu ja ne toimivat kuten on tarkoitettu. Palveluiden ja tietojen saatavuuden turvaaminen on myös olennaista, eli on tärkeää että laite- ja ohjelmistoviat, rikkomukset ja ylläpitotoimet pystytään tunnistamaan ja niihin kyetään välittömästi reagoimaan. Näissä asioissa palvelinten lokitietojen seuranta on erittäin tärkeää ja sen tuleekin kuulua ylläpitäjän rutiineihin. On lisäksi pystyttävä luottamaan siihen että valtuutettu käyttäjä todella on se joka väittää olevansa ja vastaavasti verkkopalvelin on se joka väittää olevansa. Tähän vaikuttaa luonnollisesti se että käyttäjien tunnistus ja pääsynvalvonta on toteutettu huolellisesti. (Allen 2002: 23 - 25)

Päivitysten tarkoitus on korjata ohjelmistojen ja käyttöjärjestelmien toiminnallisia ongelmia, tietoturva-aukkoja sekä tuoda uusia ominaisuuksia. Päivityksiä julkaistaan useita kertoja vuodessa, riippuen ohjelmistosta ja käyttöjärjestelmästä. Päivitysten testaaminen ennen niiden laajempaa käyttöönottoa on organisaatiolle aina haasteellinen tehtävä, mutta tärkeää toiminnan jatkuvuuden kannalta. Jotkin päivitykset saattavat esimerkiksi muuttaa ohjel-

mistojen ympäristövaatimuksia, jolloin päivitys saattaa vaatia muiden ohjelmistojen päivityksiä. Tämä puolestaan saattaa häiritä organisaation tuotantoympäristöä. (Hakala ym. 2006: 165)

Windows Server Update Server (WSUS) on Microsoft-ohjelmistojen ja -käyttöjärjestelmien päivitysten hallintatyökalu, joka käyttää avukseen Windows Automatic Update Agent –ohjelmistoa päivitysten hakemiseen Windows Update-palvelusta. WSUS toimii siis käytännössä päivityspalvelimena, joka hakee Internetistä automaattisesti uudet päivitykset. Organisaation tietojärjestelmän kaikki Windows-pohjaiset ja Microsoftin ohjelmistoja sisältävät laitteet konfiguroidaan hakemaan käyttöjärjestelmän ja ohjelmistojen automaattiset päivitykset Internetin sijasta WSUS-palvelimelta. Tämä voidaan määrittellä esimerkiksi Active Directoryn Group Policy –asetuksella (ryhmäpolitiikka), joka määrittää haluttuihin ryhmiin. Toinen vaihtoehto on muokata tietojärjestelmän laitteiden rekisteritietoja, mutta tämä toimenpide vaatii jokaisen järjestelmän laitteen erillistä konfigurointia. (Hakala ym. 2006: 165 - 166)

WSUS on monipuolinen hallintajärjestelmä, joka myös mahdollistaa aiemmin mainitun päivitysten testaamisen ennen niiden jakelua organisaation laitteille. Se tarjoaa mahdollisuuksia mm. päivitysten kieltämiseen, poistamiseen ja jakeluun haluttuihin järjestelmiin. Päivitysten hallintaa helpottaa myös tarvittaessa päivitettävien laitteiden ryhmittäminen. Näin voidaan esimerkiksi jakaa haluttu päivitys sitä tarvitsevalle ryhmälle ja kieltää se muilta. (Hakala ym. 2006: 167 - 169)

Red Hat Linux –järjestelmässä vastaava hallintajärjestelmä on Red Hat Network, joka on WSUS-järjestelmän kaltainen keskitetty hallintajärjestelmä. (Hakala ym. 2006: 169 – 170.) Kuitenkaan tässä opinnäytetyössä ei Linux-pohjaisiin ratkaisuihin juurikaan paneuduta, sillä toimeksiantajan ylläpitämät järjestelmät ovat lähes poikkeuksetta Windows-pohjaisia.

## **5.6 Palomuurit**

Palomuri on kiteytettynä yhteen lauseeseen ”laitteiston ja ohjelmiston yhdistelmä, jota käytetään kahden tai useamman verkon välistä liikennettä koskevien tietoturvapoliittikkojen toteuttamiseen”. Ilman palomuuria tai väärin konfiguroidulla palomuurilla varustettu organisaatio asettaa verkkonsa ja tietoresurssinsa alttiiksi ei-toivotulle käytölle. Käytännössä mahdollinen hyökkääjä pääsee tällöin vapaasti kiinni yrityksen tietojärjestelmään ja saattaa ilkivallalla, paljastamalla luottamuksellisia tietoja, tai muilla keinoin aiheuttaa liiketoiminnan keskeytymisen. (Allen 2002: 121 - 122)

Palomuurijärjestelmän suunnitteluun kuuluu vahvasti ympäristön dokumentointi ja tietoturva vaatimusten määrittely. Tietoturva vaatimuksia määriteltäessä tulee ottaa huomioon ketkä käyttävät palveluita joita tarjotaan Internetiin ja joita aiotaan käyttää Internetistä, palomuurin suorituskyky ja luotettavuus, kuka hallinnoi palomuuria ja miten sitä hallinnoidaan, sekä minkälaiseen järjestelmien kasvuun palomuurijärjestelmän on varauduttava. Sen jälkeen voidaan alkaa valita palomuurin arkkitehtuuria ja suodatustoimintoja. Kun nämä asiat ovat selvillä, voidaan määritellä käyttöoikeudet niille, joilla on ensisijaisesti tarve palomuurin konfigurointiin. Lopulta päästään asentamaan palomuuuri testi ympäristöön, konfiguroimaan IP-reititys ja suodatustoiminnot sekä loki- ja hälytysmekanismit. Kun testaus on suoritettu menestyksekkäästi, voidaan palomuuuri lopulta asentaa järjestelmään. On kuitenkin muistettava ottaa varmuuskopio järjestelmästä ennen palomuurin asennusta viikatilanteiden varalle. (Allen 2002: 124 - 181)

Suunniteltaessa palomuurijärjestelmää pienille tai keskisuurille yrityksille, on kustannustehokkain tapa suojata verkko yksikerroksisella palomuuuriarkkitehtuurilla (Basic Border -palomuuuri). Käytännössä tämä tarkoittaa sitä, että palomuuritoiminnot on asennettu yhteen verkon isäntäkoneeseen, joka on yhteydessä sekä sisä-, että ulkoverkkoon. Tätä käytetään yleisesti silloin kun ollaan yhdistämässä vain kahta verkkoa. (Allen 2002: 124)

Mikäli yhdistettävänä on useampia verkkoja, eivätkä kustannukset ole ongelma, on viisasta harkita monikerroksista palomuuuriarkkitehtuuria. Tällöin palomuuritoiminnot asennetaan joukolle isäntäkoneita, jotka kytketään sarjaan niin, että niiden väliin jää aina demilitarisoitu vyöhyke (demilitarized zone). Monikerroksinen arkkitehtuuri on tietenkin hankalampi käyttää ja toteuttaa, mutta kun tarvitaan vahvaa suojaa, se on erittäin hyvä ratkaisu. (Allen 2002: 124)

Suositteluvia suodatustoimintoja palomuurijärjestelmässä ovat pakettisuodatus, tilallinen pakettisuodatus sekä läpinäkyvä välityspalvelin. Paras menetelmä on näiden kolmen yhdistelmä. Pakettisuodatuksen suodatussäännöt perustuvat pakettien otsikkotietoihin, kuten lähettäjän ja vastaanottajan osoite, protokolla tai portti. Pakettisuodatuksen käyttö riittää www- ja sähköpostipalvelimen turvaamiseen. Pakettisuodatus on suorituskyvyltään tehokkain, mutta sen konfigurointi voi olla raskasta ja vaatii tarkkaa protokollien tuntemusta. Palomuurilaitteen on myös toimittava reitittimenä käytettäessä pakettisuodatusta tai tilallista pakettisuodatusta. (Allen 2002: 127 - 129)

Tilallinen pakettisuodatus tarjoaa paremmat palomuurominaisuudet kuin pakettisuodatus. Tilallinen pakettisuodatus tarkoittaa ky-

kyä käyttää paketin ulkopuolista informaatiota sisällön tutkimisen sijaan. Yhteyttä avattaessa tutkitaan ensin onko yhteys sallittu, sen jälkeen tilallinen pakettisuodatus seuraa avoimna olevia TCP- ja UDP-yhteyksiä ja sallii vain niihin kuuluvat paketit. Esimerkiksi DNS-palvelin käyttää UDP-protokollaa, joka on tilaton. Tällöin yhteyden tilaa ei voida päätellä yhdestä UDP-paketista samoin kuin TCP-paketista. Tässä tapauksessa on siis turvaututtava tilalliseen pakettisuodatukseen. (Allen 2002: 130)

Välityspalvelin toimii niin, että muodostettaessa yhteyttä asiakas-kone pyytää välityspalvelinta muodostamaan yhteyden kohdepalveluun. Pyynnön toteutuessa muodostetaan yhteys asiakkaan ja välityspalvelimen välille, sekä välityspalvelimen ja kohdepalvelun välille. Välityspalvelin on hitaampi, mutta turvallisempi kuin pakettisuodatus. Läpinäkyvässä välityspalvelimessa yhdistyvät niin pakettisuodatus, pakettien uudelleenkirjoitus kuin sovellusvälityspalvelinkin. Kun pakettiotsikko täyttää tietyn ehdon, se kirjoitetaan uudelleen niin että se ohjautuu välityspalvelimelle. Tämän ansiosta asiakaskoneen ei tarvitse antaa sovellukselle välityspalvelimen osoitetta. Asiakaskone ei myöskään voi kiertää välityspalvelinta, vaan liikenne ohjataan aina sen kautta. Välityspalvelimen lokitiedoisiin kertyvät tiedot joiden avulla voidaan seurata esimerkiksi www-sivuja joilla käyttäjät ovat käyneet. Näin ollen läpinäkyvällä välityspalvelimella voidaan myös estää pääsy ei-toivotuille sivustoille. (Allen 2002: 129 - 132)

Nyrkkisääntönä palomuurin suodatuksen konfiguroinnissa on yleisesti ”salli vain toivotut palvelut, kiellä muut”. Käytännössä potentiaalisia palveluita on kuitenkin olemassa niin paljon, että on lähes mahdotonta sanoa jokaisesta erikseen mikä on toivottua ja mikä ei. Yksinkertaisinta on tässä tapauksessa kääntyä loppukäyttäjien puoleen, he varmasti tietävät mitä palveluita tarvitsevat ja mitä eivät, vaikka eivät protokollista mitään ymmärtäisikään. Tämän lähestymistavan avulla sallitaan palvelut joita käyttäjät todella tarvitsevat ja kielletään kaikki muu liikenne. Jatkossa kun loppukäyttäjät tarvitsevat uusia palveluita, he varmasti osaavat kääntyä ylläpitäjän puoleen ja pyytää käyttöönsä palveluita tarpeen mukaan, tai ainakin varmasti valittavat jos jokin ei toimi. Kun suodatussäännöt on saatu konfiguroitua on vielä dokumentoitava ne siten, että kuka tahansa ymmärtää miten kukin suodatussääntö toimii. Tämä saattaa olla aikaa vievä toimenpide, mutta on tärkeää organisaation tietojärjestelmien toiminnan jatkuvuuden kannalta. (Allen 2002: 150 - 151, 154)

Yksi palomuurin tärkeä ominaisuus on kerätä lokitietoa verkkoliikenteestä ja palomuurin toiminnasta. Tärkeistä tapahtumista on hyvä saada reaaliaikainen hälytys, jotta mahdollisiin ongelmiin voidaan reagoida nopeasti ja organisaation toimintaa vaarantamat-



ta. Palomuurijärjestelmään onkin syytä konfiguroida loki joka tallentaa lähtevien ja saapuvien pakettien tiedot, eli paketit jotka on hylätty tai päästetty läpi. Lisäksi palomuurin toiminnasta on erittäin tärkeää olla olemassa erillinen loki joka kerää tietoa palomuuriohjelmiston käytöstä ja järjestelmästä. Palomuuriohjelmistoon on mahdollista luoda erilaisia hälytyksiä, esimerkiksi jos palomuurilaitteen levy on täyttymässä, on mahdollista luoda hälytys joka lähettää automaattisesti viestin sähköpostitse tai tekstiviestin avulla ylläpitäjälle. Näin ylläpitäjä pystyy reagoimaan tilanteeseen ja korjaamaan sen ennen kuin organisaation järjestelmälle koituu vahinkoa. Hälytyksiä on syytä konfiguroida ainakin epäonnistuneista sisäänkirjautumisyrytyksistä palomuurijärjestelmään, pakettisuodattimen muutoksista tai käytöstä poistamisesta, palomuurijärjestelmän tärkeisiin tiedostoihin kohdistuneista muutoksista sekä käyttöön liittyvistä tapahtumista, kuten loki täynnä, muisti- tai levytila vähissä ja järjestelmän uudelleenkäynnistys. Syy hälytyksien ja lokien käyttöön on järjestelmän toiminnan jatkuvuuden turvaaminen keskeytyksettä ja ilman häiriöitä. Lokit ovat myös tärkeitä työkaluja kun on tarpeen seurata suodatussääntöjen toimintaa. (Allen 2002: 157 - 160)

Palomuurijärjestelmä on syytä suojata vahvasti ei-toivotulta käytöltä. Mikäli järjestelmää on tarvetta etäkäyttää, on viisasta käyttää vahvaa tunnistusta ja hallinnollisen liikenteen salausta väärinkäytön ehkäisemiseksi. Kertakäyttöiset salasanat ovat tehokas keino palomuurin ylläpitäjän tunnistukseen. (Allen 2002: 138)

Toimeksiantajalla on yleisesti käytössään kertakäyttöiset salasanat palvelimilla jotka vaativat vahvaa tunnistusta, eli kyseessä on taskukokoinen elektroninen laite joka antaa aina kirjauduttaessa uuden salasanan ylläpitäjälle. Etäkäyttö on tässä tapauksessa välttämätöntä, sillä lähtökohtaisesti asiakkaan palomuuuri sijaitsee eri toimipisteessä kuin palomuurin ylläpitäjä.

Käyttöoikeudet palomuurijärjestelmään on erityisesti palomuurijärjestelmässä rajattava tarkasti valituille henkilöille. Käytännössä vain toimeksiantajalla on käyttöoikeus asiakkaan palomuurijärjestelmään. Lisäksi fyysistä kulunvalvontaa ei luonnollisesti tässäkin tapauksessa saa unohtaa. (Allen 2002: 138)

Palomuurijärjestelmän asennuksessa on syytä muistaa sama seikka, joka koskee myös palvelinasennuksia. Eli järjestelmään asennetaan pienin mahdollinen kokoonpano. Asennuksen jälkeen poistetaan kaikki ne palvelut tai ohjelmistot joita ei tarvita. Tällaisia palveluita ovat esimerkiksi oletuskonfiguraatioon sisältyvät X Windows-palvelut, telnet, Unix-käyttöjärjestelmissä NFS ja Windows NT –käyttöjärjestelmissä NetBIOS. Tämän jälkeen on vielä syytä ajaa kaikki mahdolliset korjaukset ja päivitykset käyttöjärjes-

telmään ja palomuuriohjelmistoon testausympäristössä ja vasta sen jälkeen asentaa palomuri järjestelmään. (Allen 2002: 145)

### 5.7 Virustorjunta

Virustorjuntaohjelmisto on virusten tartunnan estämisen perusedellytys. Useimmissa organisaatioissa virustorjunnasta on huolehdittu moitteettomasti, vaikka muihin tietoturvallisuuden osa-alueisiin ei olisikaan kiinnitetty erityistä huomiota. Virustorjuntaohjelmistoja on markkinoilla useita erilaisia. Lieneekin lähinnä makuasia mitä ohjelmistoa käytetään. (Miettinen 1999: 189 – 190.) Toimeksiantajan käytössä on F-Securen virustorjuntaohjelmisto, joten sitä myydään myös laajalti asiakasorganisaatioille.

F-Secure Client Security –ohjelmisto suorittaa määritellyistä asetuksista riippuen reaaliaikaista virustarkistusta, saapuvan ja lähtevän sähköpostin virustarkistusta, sekä verkkoliikenteen tarkistusta. Ohjelmisto antaa mahdollisuuden tehdä myös ajoitettuja virustarkistuksia, sekä manuaalisia virustarkistuksia. Yleisesti työasemassa käytetään reaaliaikaista-, sekä sähköpostin virustarkistusta. Verkkoliikenteen tarkistus tarkoittaa lähinnä palomuuritoimintoja, joille ei ole tarvetta sisäverkossa joka on suojattu palomuurilla. Sen sijaan kannettavissa tietokoneissa jotka kirjautuvat usein vieraisiin järjestelmiin, käytetään yleensä verkkoliikenteen tarkistusta. Kyseiset toiminnot voidaan määrittää joko laitekohtaisesti tai keskitetysti. Lähtökohtaisesti virustorjuntaohjelmistojen hallinta suoritetaan keskitetysti. (F-Secure jälleenmyyjäkoulutus 2006: 40)

Olennaisinta virusten torjunnassa kuitenkin on, että ohjelmistosta riippumatta virusturva pidetään ajan tasalla säännöllisillä päivityksillä. Päivityksiin kuuluvat mm. virustietokannat, jotka kertovat ohjelmistolle kaikki tunnetut virukset. Näin ollen virustorjuntaohjelma tunnistaa löytämänsä viruksen virustietokannassa olevan tiedon perusteella. (Miettinen 1999: 190)

Tärkeää on myös että ylläpitäjä valvoo jatkuvasti virustorjuntaohjelmistojen päivityksiä ohjelmiston lokitiedoista. Näin huomataan välittömästi työasemat joiden virustorjuntaohjelmistot eivät ole esimerkiksi päivittyneet ja tilanteeseen osataan reagoida vaaditulla tavalla. (Miettinen 1999: 189 - 190)

Virustorjuntaohjelmistojen hallinta ja päivitys työasemakohtaisesti on erittäin työlästä. Lisäksi se aiheuttaa huomattavaa liikenteen kasvua organisaation verkossa jos jokainen virustorjuntaohjelmisto joutuu erikseen hakemaan tietoturvapäivitykset Internetistä. Tämän vuoksi opinnäytetyössäänkin lähdetään siitä näkökulmasta, että niin käyttöjärjestelmien-, kuin tietoturvaohjelmistojenkin päivityksessä käytetään keskitettyä hallintaa.

Tämä käytännössä tarkoittaa sitä, että järjestelmään asennetaan keskitetyn hallinnan palvelin, joka hakee tietoturvapäivitykset Internetistä ja jakelee ne sen jälkeen työasemiin. Näin estetään tietoverkon ruuhkautuminen ja tietoturvaohjelmistojen hallinnasta tulee ylläpitäjälle helpompaa. (Hakala ym. 2006: 170 - 171)

Toimeksiantajan laajassa käytössä olevan F-Secure - tietoturvaohjelmiston hallinta onnistuu keskitetysti F-Secure Policy Managerilla. Järjestelmällä on mahdollista hoitaa päivitysten jakelu organisaatiossa keskitetysti, sekä hallita ohjelmiston asetuksia. Järjestelmään kuuluvia komponentteja ovat *Policy Management Server*, joka on keskitetyn hallinnan palvelin ja käyttää apunaan mukana toimitettavaa Apache-WWW -palvelinta. *Policy Management Console*, joka on hallintapalvelimen pääkäyttösovellus. *Update Agent*, joka hakee päivityksiä Internetistä hallintapalvelimelle. *Management Agent* on hallittavien sovellusten komponentti, joka keskustelee hallintapalvelimen kanssa.

Management Console –pääkäyttösovelluksen avulla voidaan mm. asentaa tietoturvaohjelmistot haluttuihin työasemiin erikseen (push-install), tai kaikkiin kerralla (autodiscover). Sen avulla päästään lisäksi muokkaamaan virustorjunta-asetuksia, hallitsemaan haittaohjelmistojen suojausjärjestelmää sekä määrittelemään palomuuriohjelmiston asetuksia.

Järjestelmä sisältää myös raportointijärjestelmän, joka välittää viruksen tai muun poikkeavan tilanteen löytyessä hälytyksen Management Agentin avulla hallintapalvelimelle. Hallintapalvelimelta pääkäyttäjää pääsee seuraamaan organisaation tietoturvaohjelmistojen toimintaa ja mm. päivitysten asennusta reaaliajassa. (Hakala ym. 2006: 171 - 173)

## 5.8 Ohjelmistoturvallisuus

Ohjelmistoturvallisuuteen kuuluu mm. ohjelmistojen testaus, niiden sopivuus suunniteltuun käyttötarkoitukseen, ohjelmistojen keskinäinen yhteensopivuus, toiminnan luotettavuus ja virheettömyys, sekä ohjelmistoversioiden ja lisenssien hallinta. (Hakala ym. 2006: 11 – 12.) Vastuu ohjelmistojen turvallisuudesta on tässä tapauksessa toimeksiantajalla, joka tekee ohjelmistojen asennukset asiakasorganisaatiolle. Näistä osa-alueista ainoastaan ohjelmistojen sopivuus suunniteltuun käyttötarkoitukseen on alue, joka käydään läpi asiakasorganisaation kanssa. Lähinnä siis toimeksiantaja pyrkii etsimään asiakkaan tarpeisiin ja vaatimuksiin parhaiten soveltuvat ohjelmistot.

Ohjelmistoturvallisuuden toteuttamiseen kuuluvat myös ohjelmistojen pääsynvalvonta, tapahtumatietojen seuranta, varmuuskopi-

ointi, ohjelmistodokumentaatio, ylläpito- ja huoltosopimukset, sekä ohjelmistojen laillisuudesta, eli rekisteröityjen ohjelmien käytöstä huolehtiminen. (Miettinen 1999: 224 - 228)

Kuten huomataan, ohjelmistoturvallisuus käsittää samoja osa-alueita ja menetelmiä kuin monet muutkin aiemmin käsitellyt asiat. Näitä osa-alueita on siis käsitelty ja tullaan käsittelemään tässä opinnäytetyössä vielä myöhemmin, näin ollen aikaisempien asioiden toistaminen ei liene järkevää tässä yhteydessä. Toisin sanoen ohjelmistoturvallisuus on laajuutensa vuoksi hajautettu tässä opinnäytetyössä useisiin eri lukuihin. Ohjelmistojen pääsynvalvonta toteutetaan käyttäjätunnuksilla, joita käsitellään henkilöstöturvallisuutta koskevassa luvussa. Tapahtumatietojen seuraaminen tarkoittaa käytännössä lokien seurantaa jota on käsitelty tässä luvussa aiemmin, samoin kuin dokumentaatiota. Varmuuskopiointia tullaan käsittelemään tarkemmin myöhemmin tässä luvussa. Ylläpito- ja huoltosopimukset eivät liene tässä tapauksessa olennaisia, sillä asiakasorganisaatiolla nimenomaan on ylläpitosopimus toimeksiantajan kanssa. Tilanteissa joissa käytetään toimeksiantajalle tuntemattomampia tai muuten vahvaa osaamista vaativia ohjelmistoja, voidaan solmia ohjelmiston hankinnan yhteydessä ylläpito- ja huoltosopimus ohjelmiston myyjän kanssa. Monesti ohjelmistoa ostettaessa myyjä lupaakin jonkin tietyn ylläpitoajan. Mikäli jatkossa tarvitaan ulkoista ylläpitoa, siitä sovitaan erikseen.

Näin ollen tässä yhteydessä ainoa erityisesti ohjelmistoturvallisuuteen liittyvä tärkeä seikka on rekisteröityjen ohjelmistojen käytöstä huolehtiminen. Käytännössä siis organisaatiossa käytettävien ohjelmien tulee olla laillisia. Ohjelmistot ovat valmistajansa omaisuutta, joten organisaatio joutuu helposti rikosoikeudelliseen vastuuseen laittomien ohjelmistojen käytöstä. Tämän vuoksi ylläpitäjän tulee olla tarkkana organisaatiossa käytettävien ohjelmistojen laillisuudesta ja puuttua tarpeen mukaan väärinkäytöksiin. (Miettinen 1999: 228.) Toimeksiantajakin on omalta osaltaan vastuussa asentamiensa ohjelmistojen laillisuudesta, joten kaikki yritykseen hankittavat ohjelmistot hankitaan vain virallisen toimittajan kautta. Tällöin laittomia ohjelmistoja ei pääse kulkeutumaan asiakasyrityksiinkään.

## **5.9 Tietoaineistoturvallisuus**

”Tietoaineistoturvallisuuteen kuuluvat tietojen säilyttämiseen, varmistamiseen ja palauttamiseen, sekä tuhoamiseen liittyvät toimenpiteet” (Hakala ym. 2006: 11). Asiakasyrityksen vastuulle jäävät tässä tapauksessa luonnollisesti manuaalisen tietojenkäsittelyn asiakirjat sekä tulosteet. Tietojen tuhoamista, joka myös kuuluu osittain tietoaineistoturvallisuuteen, on käsitelty aiemmin fyysistä turvallisuutta koskevassa luvussa.

Kuten aiemmin fyysistä turvallisuutta koskevassa luvussa on todettu, lähtökohtaisesti palvelun tuottaja vastaa lisenssien ja asennusmedioiden säilyttämisestä. Palvelujen tuottajan on vikatilanteessa saatava käsiinsä tarvittavat asennusmediat vaivattomasti, joten tämän vuoksi on viisasta säilyttää niitä palvelujen tuottajan toimesta. Sama koskee pidempään säilytettäviä varmuuskopioita.

Tietoaineistoturvallisuudella halutaan myös varmistaa, että tiedot pysyvät vain niillä henkilöillä jotka niitä työhönsä tarvitsevat. Perustan sen toteutukselle muodostaa tietojen turvaluokitusjärjestelmä. (Miettinen 1999: 22 - 23)

### **5.9.1 Tiedon luokittelu (Miettinen 1999: 241 - 246)**

Organisaation luottamuksellisten tietojen joutuminen väärin käsiin voi johtaa väärinkäyttöön ja sitä kautta aiheuttaa taloudellisia, oikeudellisia tai yhteiskunnallisia seuraamuksia organisaation toiminnalle. Jokaisen henkilön jolla on pääsy organisaation tietoihin, on ymmärrettävä tietojen sisällön arvo, jotta niitä voidaan käsitellä oikein tiedon elinkaaren jokaisessa vaiheessa.

Oleennaista tietojen turvaluokitusjärjestelmän suunnitteluvaiheessa on organisaation toiminnassa käytettävien tietotyyppien tunnistaminen. Niistä strategiset tiedot ovat tärkeimpiä suoranaisesti organisaation toimintaan liittyviä tietoja. Niihin kuuluvat mm. johtoportaan muistiot, henkilöstömäärät ja omistussuhteet, tuotantoteknologiaa koskevat suunnitelmat ja ennusteet, liiketaloudelliset suunnitelmat, sekä riskienhallintaan liittyvät tiedot. Muita tietotyyppejä voivat olla asiakassuhteisiin, henkilöstöön, tuotekehitykseen, sekä tuotteisiin ja palveluihin liittyvät tiedot. Erityisesti tässä yhteydessä on kiinnitettävä huomiota turvajärjestelyihin liittyviin tietoihin, jotka ovat ehdottomasti salassa pidettäviä. Poikkeuksena tietenkin turvajärjestelyjen olemassaolosta kertovat julkisuuteen annettavat tiedot.

Tietojen turvaluokitusjärjestelmän periaatteena on merkitä organisaation tiedot järjestelmällisesti, jotta tiedon sisällön merkitys selviää organisaation henkilöstölle ja sidosryhmille. Tarkoituksena on luokitella kaikki ne tiedot joiden sisältö sitä edellyttää ja luoda tärkeysluokkiin kuuluville tiedoille omat käsittelysäännöt. Luokitusääntöihin kuuluu kaikkia muodoissa tallennetut tiedot, niin palvelimille tallennettu data kuin paperitulosteetkin.

Suomessa ei ole varsinaisia velvoitteita organisaation turvaluokituskäytännöstä, mutta lait ja asetukset on ehdottomasti otettava huomioon luokitusääntöjä mietittäessä. Laki velvoittaa yrityksen

pitämään esimerkiksi henkilötietoja sisältävät dokumentit salassa, joten luokitus säännöissä tähän tulee ottaa kantaa.

Luokitusjärjestelmää käyttämällä organisaatio voi tehostaa toimintaansa, varautua tietojen väärinkäyttöön, vähentää kustannuksia, motivoida henkilöstöä ja kehittää yrityskuvaansa myönteisesti. Jos kaikkia tietoja käsitellään samalla tavalla, jotkin tiedot jäävät liian vähälle suojaukselle, toisia taas suojataan liiankin tehokkaasti. Tällöin organisaatiolle saattaa koitua ylimääräisiä kuluja ja ylimääräistä työtä. Luokitus säännöillä pystytään myös väärinkäyttötapauksissa osoittamaan väärinkäytettyjen tietojen tärkeys tuomioistuimessa. Luokittelu myös ehkäisee ennalta väärinkäyttöä, koska potentiaalinen väärinkäyttäjä tietää luokiteltujen tietojen väärinkäytön johtavan todennäköisesti oikeudellisiin seuraamuksiin. Lisäksi henkilöstö oppii ymmärtämään luokittelusääntöjen avulla käsittelemänsä tiedon arvon, eikä näin ollen ainakaan tahattomasti paljasta luottamuksellista tietoa.

Tietojen turvaluokitus säännöissä määritellään ensin tiedon omistaja ja haltija. Omistaja on yleensä tiedon luoja, jonka velvollisuus on luokitella ja merkitä tieto turvaluokitus käytännön mukaan. Tiedon haltija puolestaan on velvollinen käsittelemään tietoa luokitus käytännön mukaisesti.

Itse tiedot luokitellaan yleisimminkin neljään pääluokkaan: julkinen, sisäinen, luottamuksellinen ja salainen. Julkisia tietoja ei yleensä merkitä, eikä niiden käsittelyssä tai tallentamisessa ole rajoituksia. Sisäiset tiedot ovat yrityksen henkilöstölle tarkoitettuja tietoja, joiden joutuminen ulkopuolisen käsiin ei ole vaarallista. Luottamukselliset tiedot eivät ole tarkoitettu kaikkien yrityksen työntekijöiden käytettäväksi ja niiden käyttö ja säilyttäminen vaatii tiedon omistajan luvan. Sama pätee pitkälti salaisiin tietoihin, joka on luokitus säännösten vahvimmin rajoitettu luokitus. Viime kädessä luokittelukäytäntö riippuu kuitenkin aina organisaation tarpeista, joten tietojen luokittelu ja käsittelysäännöt muokataan kussakin organisaatiossa tarkoituksiin sopiviksi.

Asiakasorganisaation tietojen luokittelujärjestelmän suunnittelu ja käyttöönotto on luonnollisesti asiakasorganisaation vastuulla. Sitä ei kuitenkaan voi tässä tapauksessa täysin sivuuttaa, sillä ylläpitäjä joutuu työssään väistämättä käsittelemään asiakasorganisaation turvaluokituksen alaista tietoa, tai päinvastoin. Näin ollen sekä asiakkaan että ylläpitäjän on tahallisen ja tahattoman väärinkäytön estämiseksi oltava tietoisia luokittelujärjestelmään kuuluvien tietojen luokitteluperusteista ja käsittelytavoista.

## 5.9.2 Varmuuskopiointi

Varmuuskopioinnilla varmistetaan, että yrityksellä on käytössään jatkuvasti ajantasaiset varmuuskopiot tietoaineistosta ja järjestelmästä. Mikäli tiedostot syystä tai toisesta katoavat, tai järjestelmä rikkoutuu, voidaan se palauttaa viipymättä ilman merkittäviä liiketoiminnallisia haittoja. Mikäli käytettävissä ei ole varmuuskopioita, toimenpide saattaa olla mahdoton varsinkin tiedostojen osalta ja lisäksi järjestelmän uudelleen asennus kestää huomattavasti kauemmin kuin järjestelmän palautus varmuuskopiolta. Tällöin liiketoiminnalle saattaa aiheutua erittäin merkittäviä taloudellisia haittoja. (Miettinen 1999: 239)

Palvelinten varmistaminen kuuluu jokaisen organisaation tietojärjestelmän peruspilareihin. Luonnollisesti toimiva varmistusjärjestelmä vaatii että kaikki organisaation data on tallennettu keskitetysti palvelimille, kuten jo opinnäytetyön henkilöstöturvallisuutta käsittelevässä luvussa kävi ilmi. Varmistusjärjestelmän suunnitteluun, toteutukseen ja testaukseen tulee panostaa, sillä vikatilanteessa organisaation tietojen säilyminen on vahvasti riippuvainen varmistusjärjestelmästä. (Hakala ym. 2006: 141)

Toimiva varmistuskäytäntö on, että järjestelmän sisältämä data varmistetaan usein ja käyttöjärjestelmä asetuksineen ja ohjelmistoineen harvoin. (Hakala ym. 2006: 142 – 143.) Toinen toimiva ja toimeksiantajan laajalti käyttämä varmistusjärjestelmä on, että niin ikään järjestelmän sisältämä data varmistetaan usein ja jokainen palvelin sisältäen käyttöjärjestelmän, ohjelmistot sekä datan varmistetaan harvoin. Se kuinka usein tai harvoin varmistuksia otetaan on täysin riippuvainen organisaation tarpeista. Yleinen käytäntö toimeksiantajalla on, että palvelinten sisältämä data varmistetaan päivittäin ja koko järjestelmän kaikkien palvelinten varmuuskopio otetaan jokaisen viikon perjantaina.

Nykyaikana varmistusjärjestelmä on useimmiten automatisoitu järjestelmä joka ottaa varmuuskopiot määrättyinä aikoina automaattisesti. Usein ainoa manuaalinen tehtävä varmistusten ylläpitämisessä onkin varmistusmedian vaihtaminen. Vastaava järjestelmä on myös laajassa käytössä toimeksiantajalla. Mikäli kuitenkin järjestelmään tehdään suuria muutoksia, on viisasta ottaa koko järjestelmästä manuaalisesti varmuuskopio ennen muutosten toteuttamista. Palautuksen kannalta on otettava huomioon, että esimerkiksi käyttöjärjestelmän rikkoutuessa, se voidaan palauttaa nopeasti toimintaan mikäli fyysinen laitteisto pysyy samanlaisena. Ohjelmistot pystytään palauttamaan mikäli käyttöjärjestelmä on pysynyt samanlaisena, pelkän ohjelmiston palauttaminen erikseen on miltei mahdotonta. Data puolestaan voidaan palauttaa jos ohjelmistot tu-

kevat datan varmistettua muotoa. Mikäli ennen palauttamista on tehty ohjelmistopäivitys, vanha data ei välttämättä tue uutta ohjelmistoa, eikä palautus onnistu. (Hakala ym. 2006: 143)

Yleisimmin eheyden ja saatavuuden ongelmat liittyvät tiedon tuhoutumiseen tai muuttumiseen. Palvelinjärjestelmän tuhoutuminen on harvinaisempaa ja liittyy laitteiden rikkoutumiseen. Näin ollen palautusprosesseissa käsitellään useimmiten dataa. Itse järjestelmän tuhoutuminen tai korruptoituminen voidaan parhaiten estää testaamalla ohjelmisto- ja käyttöjärjestelmäpäivitykset ennen laitteen käyttöönottoa. (Hakala ym. 2006: 146)

Yleisimmin käytettyjä varmistusmedioita ovat CD, DVD, ulkoinen kiintolevy, varmistusnauha tai nauharobotti. CD ja DVD ovat kustannuksiltaan halvimmat, mutta myös tallennuskapasiteetiltaan pienimmät vaihtoehdot. Niiden kapasiteetti liikkuu 650 Megatavun (tavallinen CD-R) ja 17 Gigatavun (nelikerroksinen DVD) välillä. Näitä käytettäessä saattaa järjestelmän kasvaessa eteen tulla tilanne, ettei koko järjestelmän data mahdu medialle. CD ja DVD ovatkin näin ollen käyttökelpoisia varmistusmedioita vain pienyrityksissä joissa varmistettavan datan koko ei ylitä CD:n tai DVD:n kapasiteettia ja joissa halutaan hoitaa varmistukset halvimmillä mahdollisilla kustannuksilla. Ulkoinen kiintolevy on myös yksi vaihtoehto jonka kapasiteetti voi olla jopa teratavuja. (Hakala ym. 2006: 144)

Toimeksiantajan käytössä yleisimpiä ovat kuitenkin varmistusnauhat. Nauharobotteja käytetään joissakin yrityksissä ja ne antavatkin käyttöön suurimman mahdollisen kapasiteetin joka voi parhaimmillaan olla useita teratavuja. Nauharobottien kustannukset liikkuvat kuitenkin niin korkealla, ettei pienemmän yrityksen ole järkevää panostaa niihin. Nopean hintavertailun tuloksista todettakoon sen verran, että esimerkiksi Multitronic Webshop –verkkokauppa ([www.multitronic.fi](http://www.multitronic.fi)) myy Tandberg LTO Autoloader Desktop –nauharobottia hintaan 7536,67 € (6.3.2007). Turkulainen DataInfo Solutions –jälleenmyyntiyritys ([www.datainfoturku.com](http://www.datainfoturku.com)) myy HP Compaq DAT72 AE350AT –merkkistä ulkoista nauha-asemaa hintaan 625 € (6.3.2007). Vertailu kertoo kiistatta nauharobottien nauha-asemien hintaeron, joten yritykset varmasti mieluusti turvautuvat nauha-asemiin.

Yleisimmin käytössä olevien varmistusnauhojen kapasiteetti voi olla satoja gigatavuja, jolloin pienempi organisaatio tulee varmasti pitkälti toimeen varmistusnauhoja käyttämällä. Järjestelmän kasvaessa voidaan varmistustehtäviä jakaa useammallekin palvelimelle jolloin kapasiteetti moninkertaistuu, mutta kustannukset pysyvät silti huomattavasti nauharobottin vaatimaa panostusta alhaisempina. (Hakala ym. 2006: 144)



Varmistuskierto määrittelee varmistusten ajankohdan, varmistustavan, varmistusmedioiden kierron ja varmistusnauhojen säilytysajan. Tietojen varmistus vaatii toteutushetkellä huomattavasti verkkoresursseja, joten varmistus on järkevää suorittaa ajankohtana jolloin verkossa ei ole juurikaan muuta liikennettä tai käynnissä muita prosesseja. Tämä senkin vuoksi että mikäli tiedot ovat käytössä varmistuksen aikana, niitä ei pystytä varmistamaan. Viisain aika varmistukseen onkin yö, olettaen että organisaatiossa työskennellään klo 7 ja klo 20 välisenä aikana kuten yleisimmin. Suositeltavin varmistuksen kierto kulkee viikoittain niin, että sunnuntain ja maanantain välisenä yönä otetaan järjestelmästä palvelimien täydellinen varmuuskopio. Tähän kopioon varmistetaan päivittäin muuttunut data ja nauha vaihdetaan aina uuteen viikon viimeisen varmistuksen jälkeen. Nauhojen säilytysajat vaihtelevat niiden sisältämän datan mukaan, mutta suositellaan että kolmen kuukauden välein otetaan talteen kuukauden ensimmäisen viikon täydellinen varmuuskopio ja sitä säilytetään yksi vuosi. Nauha nimetään vuoden ja kuukauden mukaan. Lisäksi jokaisen vuoden viimeistä täydellistä varmistusnauhaa suositellaan säilytettäväksi kaksi vuotta. Nauha nimetään vuoden mukaan. Edellinen kierto on kuitenkin lähinnä suositus josta selviää varmistuskierron periaatteet. Varmistus on aina organisaatiokohtainen asia, joten sen toteutus riippuu täysin organisaation tarpeista. (Hakala ym. 2006: 145)

Varmuuskopionauhojen vaihtamisesta vastaa asiakas, joten myös varmuuskopioiden säilyttäminen jää asiakkaan vastuulle. Nauhojen turvallista säilyttämistä on käsitelty aikaisemmin opinnäytetyön tietojen säilyttämistä koskevassa luvussa, jossa käsiteltiin säilytystilaan kohdistuvia fyysisiä uhkia ja varmistusnauhojen suojaamista niiltä. Tässä tapauksessa on kuitenkin otettava huomioon myös se, että vikatilanteessa palvelujen tuottaja suorittaa vaadittujen tietojen palauttamisen, jolloin varmuuskopioiden pitää olla palvelujen tuottajan saatavilla viipymättä.

Säilytysaikaan liittyen on myös otettava huomioon lain määrittelemät vaatimukset vanhan tiedon säilyttämisestä. Vaadittu säilytysaika vaihtelee tiedon luonteen ja sitä koskevien lainkohtien mukaan. Säilytysajan määrittelystä sekä säilytyksen toteuttamisesta huolehtii luonnollisesti asiakasyritys. Ylläpitäjän kannalta on ainoastaan olennaista että saatavilla on jatkuvasti ajankohtainen varmuuskopio järjestelmästä sekä datasta. (Hakala ym. 2006: 144)

Organisaation on syytä päättää varmuuskopioinnista vastaavat henkilöt, jotka käytännössä hoitavat päivittäin varmistusnauhojen vaihtamisen, merkitsemisen ja toimituksen säilytykseen. Vastuullisten henkilöiden koulutuksesta ja ohjeistuksesta tulee myös huolehtia niin, että minimoidaan vastuuhenkilöiden toiminnasta aiheu-

tuneet riskit. Koulutus ja päivittäinen varmuuskopiointiin käytettävä työmäärä on organisaatiolle pieni panos suhteutettuna ammattitaidottoman henkilön tuomiin riskeihin varmistuksen yhteydessä tai tietojen varmistuksen unohtamiseen.

Palvelujen tuottaja seuraa varmuuskopiointiin onnistumista varmuuskopiointiohjelman lokitiedostoista viikoittain, aivan kuten palvelinten ja palomuurien lokitiedostojakin. Näin kyetään viipymättä huomaamaan ongelmat varmuuskopiointissa, kuten nauhaseman rikkoutuminen, tai varmuuskopiointia muuten häiritsevät tekijät.

Työaseman varmistusta helpottava tekijä on keskitetty datan tallentaminen. Kun yrityksessä on käytössä palvelin, ei ole järkevää säilyttää dataa itse työasemissa. Windows-järjestelmässä on kuitenkin syytä muistaa ohjata työasemien Omat tiedostot, eli My Documents –hakemistot palvelimelle jaettuun kansioon. Käyttäjillä on usein tapana suosituksista huolimatta tallentaa henkilökohtaista tietoa omalle työasemalleen, joten kun käyttäjän omat tiedostot on ohjattu palvelimelle, ei tarvitse huolehtia tiedon menetyksestä työasemalta mahdollisen laiterikon sattuessa. (Hakala ym. 2006: 146)

Työaseman asennusvaiheessa on viisasta tehdä työasemasta esimerkiksi CD:lle tai DVD:lle työaseman kuva, eli niin sanottu image. Tämä voidaan tehdä useilla eri ohjelmilla, joista ehkä yleisin ja näin ollen mainitsemisen arvoinen on Norton Ghost. Mikäli työaseman kokoonpanoa tai ohjelmistoja muutetaan on järkevää myös tehdä uusi image. Mahdollisen laiterikon sattuessa vioittuneet osat voidaan korvata uusilla alkuperäistä vastaavilla osilla ja palauttaa työasema imagelta. Palauttaminen kestää työaseman tehosta riippuen muutamista minuuteista muutamiin tunteihin ja verrattuna työaseman kokonaiseen uudelleenasetukseen ajan säästö on selkeä. Työasemat kannattaa siis mahdollisuuksien mukaan standardoida, eli rakentaa niin että jokainen työasema on kokoonpanoltaan samanlainen. Näin toimittaessa voidaan palauttaa yhdeltä imagelta vaikka yrityksen jokainen työasema. Pääsääntö on tehdä organisaation jokaisesta erilaisesta kokoonpanosta oma image, niin että jatkuvasti on saatavilla ajankohtainen varmuuskopio työasemista. (Hakala ym. 2006: 146)

Usein varmuuskopiointiin luotetaan sokeasti ja oletetaan että mahdollisessa vikatilanteessa tiedon palauttaminen niiltä onnistuu mutkattomasti. On kuitenkin mahdollista että itse varmistusjärjestelmässä on jokin vika, joka estää varmuuskopioita toimimasta palautustilanteessa. Mahdollista on myös että olosuhteet joissa varmuuskopioita säilytetään, ovat vahingoksi esimerkiksi varmistuksessa käytettäville magneettinauhoille. Tällöin ne ovat pahimmassa

tapauksessa käyttökelvottomia siinä vaiheessa kun järjestelmää pitäisi alkaa palauttaa. Tämän vuoksi on viisasta ajoittain testata varmuuskopion toimivuus, eli testata että datan palauttaminen varmuuskopiolta todella onnistuu. Itse varmistusjärjestelmä kannattaa testata ennen varsinaista käyttöönottoa kuten muutkin verkon ydinlaitteet. Testausvaiheessa otetaan varmuuskopio testiympäristöstä ja sen jälkeen palautetaan. Palautuksen onnistuessa voidaan olla varmoja ainakin siitä että järjestelmä todella toimii. Toinen uhka, eli pitempiä aikaista säilytystä vaativien varmuuskopioiden varastoinnin aiheuttamat ongelmat voidaan todeta vain säännöllisellä testauksella, joka kannattaa tehdä esimerkiksi puolivuositain tai riippuen organisaation tarpeista.

## 6 Tietoturvapoliitiikan toteutus

PPCT Finland Oy:n tietoturvapoliitiikkaan päätettiin sisällyttää seuraavat kohdat:

- Tietoturvapoliitiikan kuvaus
- Tietoturvallisuuden päämäärä ja tavoitteet
- Tietoturvallisuuden määritelmä
- Organisaatioiden väliset vastuukysymykset
- Osapuolten välinen salassapito
- Osapuolia sitovat lainkohdat
- Toteutuskeinot
- Organisaatioiden välinen tiedottaminen
- Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely

Tietoturvapoliitiikkaan sisällytettiin aluksi esittelyluku, jossa kerrotaan lyhyesti mistä dokumentissa on kysymys. Seuraavaksi asetettiin tietoturvallisuuden päämäärä, joka on kiteytettynä asiakasorganisaation liiketoiminnan jatkuvuuden turvaaminen. Tavoitteiksi päätettiin ottaa myös tietojärjestelmän keskeytyksetön toiminta, luvattoman käytön estäminen, tiedon tuhoutumisen ja vääristymisen estäminen sekä riskeihin varautuminen ja niiden aiheuttamien vahinkojen minimointi. Tietoturvallisuus määriteltiin tietoturvapoliitikassa samaan tapaan kuin opinnäytetyön johdantoluvussakin.

Vastuukysymyksiä lähdettiin purkamaan tietoturvallisuuden osaluokkien mukaan. Näistä hallinnollinen turvallisuus, henkilöstö- ja toimitilaturvallisuus, fyysinen turvallisuus sekä tietoaineistoturvallisuus päätettiin sisällyttää asiakasorganisaation vastuualueisiin. Tietoliikenneturvallisuuden toteutus, ylläpito ja tekninen seuranta jätettiin toimeksiantajan vastuulle. Tämä yksinkertaisesti siitä syystä, ettei toimeksiantajalla ole mahdollisuutta asiakasorganisaation jatkuvaan hallinnolliseen seurantaan. Tärkeintä tässä yhteydessä oli se, että asiakasorganisaatio ymmärtää myös oman vastuunsa tietoturvallisuuden toteuttamisen osana.

Salassapitosopimus yhdistettiin tietoturvapoliitiikkaan, jolloin päästiin eroon erillisestä salassapitosopimuksesta. Osapuolten välinen salassapito on myös olennainen asia tietoturvallisuuden kannalta, joten se oli järkevää yhdistää tietoturvapoliitiikkaan. Myös osapuolia sitovat lainkohdat huomioitiin tietoturvapoliitikassa.

Tietoturvapoliitiikan toteutuskeinot määriteltiin vastuualueiden mukaan. Yksityiskohtaisia ratkaisuja ei luonnollisesti kirjattu poliitiikkaan, vaan pitäydettiin yleisissä osapuolia sitovissa toimintamalleissa. Osapuolten välinen tiedottaminen huomioitiin myös, joten ylläpitosopimusta kirjoitettaessa voidaan tietoturvapoliitiikkaan lisätä organisaatioiden välisestä tiedottamisesta vastaavat henkilöt.

Näin ollen asiakasorganisaation henkilöstö osaa ongelmatilanteissa kääntyä vastuuhenkilöiden puoleen.

Viimeisenä alakohtana tietoturvapoliikkaan kirjattiin tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely. Toimeksiantajan vastuulle sisällytettiin tietoturvallisuuden tekninen seuranta. Hallinnollinen seuranta jätettiin asiakasorganisaation vastuulle. Ylläpitäjä saa reagoida teknisiin ongelmiin myöhemmin sovittavien kustannuksien rajoissa. Mikäli asiakasorganisaatio itse tekee muutoksia, jotka vaikuttavat tietoturvallisuuteen, niistä on informoitava toimeksiantajaa. Nämä olivat olennaisia kohtia asiakasorganisaation tietoturvallisuuden ylläpitämiseksi. Lopulta kuitenkin jokainen käyttäjä on omalta osaltaan vastuussa tietoturvallisuuden noudattamisesta. Tämä tehtiin tietoturvapoliikassa selväksi, jotta jokainen tietojärjestelmän käyttäjä myös tietää oman vastuunsa. Lopuksi kirjattiin ylös sanktiot, joita tietoturvallisuuden rikkomisesta voi seurata. Tässä yritettiin välttää pelottelevaa ja negatiivista kirjoitustapaa, joten yksityiskohtaisia rangaistuksia ei lueteltu.

Tietoturvapoliikkaan siis sisällytettiin vaatimusten mukaiset asiat, jotka tulivat ilmi johdantoluvussa. Itse tietoturvapoliikan vastualueiden jakamisessa käytettiin vahvasti hyväksi opinnäytetyön teoriaosuutta, jonka pohjalta vastualueet oli helppo jakaa osapuolten välillä.

## 7 Yhteenveto

Opinnäytetyössäni olen käynyt läpi olennaisimmat tietoturvallisuuden vaikuttavat osatekijät. Niiden avulla olen purkanut suunnitellun tietoturvapoliitikan yleisiksi käytännöiksi ja toimenpiteiksi, joita tietoturvapoliitikan toteuttaminen todellisuudessa vaatii. Työni perustuu vahvasti PPCT Finland Oy:ssä oppimiini toimintamalleihin ja ratkaisuihin.

Lähtökohtana tälle opinnäytetyölle oli PPCT Finland Oy:n tarve yhdenmukaistetulle toimintamallille asiakkaiden ylläpitotoiminnassa. Toimintamallin pohjaksi päätin toteuttaa tietoturvapoliitikan, joka luo perustan tietoturvallisuuden toteuttamiseen ylläpitoasiakkaiden tietojärjestelmissä. Tietoturvapoliitikkaa käyttämällä samoja periaatteita voidaan noudattaa asiakkaasta riippumatta.

Omalta osaltani tahdoin selvittää tietoturvallisuuden käsitteen koko laajuudessaan niin itselle, kuin muillekin asiasta kiinnostuneille ja tietoturvallisuuden parissa työskenteleville. Erityisesti halusin kiinnittää huomiota hallinnolliseen turvallisuuteen ja henkilöstöturvallisuuteen jotka niin usein on unohdettu, etenkin kun tietojärjestelmän ylläpito on ulkoistettu.

Näistä lähtökohdista lähdin rakentamaan opinnäytetyötäni muutama lähdeoksen avulla. Projektin edetessä lähdeaineisto kasvoi lopulta valtavasti ja huomasiinkin käsitteleväni erittäin ajankohtaista aihetta. En kuitenkaan halunnut unohtaa hieman vanhempaakin aiheeseen liittyvää materiaalia, sillä se tarjosi jossain määrin sellaista tietoa, joka nykykirjallisuudesta on monesti unohdettu, mutta joka on kuitenkin vielä vartenotettavaa kattavan tietoturvallisuusratkaisun suunnittelussa. Luonnollisesti oma kokemus alalta näytteli myös vahvaa roolia projektin toteutuksen eri vaiheissa.

Mielestäni onnistuin opinnäytetyössäni hyvin huolimatta aihealueen laajuudesta. Työstä tuli lopulta suhteellisen yleislukuinen, eli lähes kuka tahansa pystyy sen ymmärtämään. Kuitenkaan työ ei ole liian yleispätevä, eli se tarjoaa myös konkreettisia ratkaisuja.

Itse tietoturvapoliitikasta onnistuin saamaan tarpeeksi yksityiskohdaisen, eli se ei jäänyt liian yleisluontoiseksi ja näin ollen hyödyttömäksi. Uskon että toimeksiantaja pystyy hyödyntämään tietoturvapoliitikkaa solmittaessa uusia ylläpitosopimuksia pienten ja keskisuurten yritysten kanssa. Tietoturvapoliitikka takaa vankan pohjan tietoturvallisuusasioiden hoitamiselle, antaa yhdenmukaiset toimintamallit ylläpitoyritysten välillä ja varmasti kasvattaa toimeksiantajan toiminnan laatua asiakasorganisaatioiden silmissä. Näin ollen koen onnistuneeni asetettujen tavoitteiden täyttämässä.

## Lähteet

Allen, Julia H. 2002. CERT - Verkkotietoturvan hallinta. Helsinki: Edita.

Arkistolaki 23.9.1994/831. [Online] [Viitattu 14.3.2007].  
<http://www.finlex.fi/fi/laki/ajantasa/1994/19940831>

Dataturvakaapit 2007. Safelock Finland Ltd Oy. [Online] [Viitattu 12.3.2007].  
[http://www.kassakaappi.fi/tuotteet/index.php?group=00000043&mag\\_nr=10](http://www.kassakaappi.fi/tuotteet/index.php?group=00000043&mag_nr=10)

Ernst & Young: Tietoturvariskejä yrityksen sisältä 2004. ITViikko 30.9.2004, 8.

Expert Eraser –käyttö 2001. Norman Ibas Oy. [Online] [Viitattu 7.3.2007].  
[http://docs.ibas.com/ee/fi\\_ee.pdf](http://docs.ibas.com/ee/fi_ee.pdf)

F-Secure jälleenmyyjäkoulutus 2006. Luentomateriaali.

F-Secure tietoturvayhteenveto, heinäkuu-joulukuu 2005. [Online] [Viitattu 7.3.2007].  
[http://www.f-secure.fi/export/system/fsgalleries/white-papers/f-secure\\_tietoturvayhteenveto\\_heinakuu\\_joulukuu\\_2005.pdf](http://www.f-secure.fi/export/system/fsgalleries/white-papers/f-secure_tietoturvayhteenveto_heinakuu_joulukuu_2005.pdf)

F-Securen tietoturvakatsaus heinä-joulukuu 2006. [Online] [Viitattu 7.3.2007]. <http://www.f-secure.fi/2006/2/>

Hakala, Mika & Vainio, Mika & Vuorinen, Olli 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Henkilötietolaki 22.4.1999/523. [Online] [Viitattu 14.3.2007].  
<http://www.finlex.fi/fi/laki/ajantasa/1999/19990523>

Hikipedia 2007. [Online] [Viitattu 15.3.2007] <http://hiki.pedia.ws/>

Hämäläinen, Pertti 2007. IP-puheen tietoturva puhuttaa. Tietokone 1/2007, 49 - 50.

Järvinen, Petteri 2003. Salausmenetelmät. Jyväskylä: Docendo.

Järvinen, Petteri 2007. 10 tapaa suojaautua roskapostilta. Tietokone 1/2007, 40 - 41.

Karjalainen 22.3.2005. Henkilöstö ja hallinto tietoturvan heikkouksia, 11.

Laki yksityisyyden suojasta työelämässä 13.8.2004/759. [Online] [Viitattu 14.3.2007].

<http://www.finlex.fi/fi/laki/ajantasa/2004/20040759>

Miettinen, Juha E. 1999. Tietoturvallisuuden johtaminen - näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari.

Miksi suojautua? 2007. Innosec Oy. [Online] [Viitattu 12.3.2007].

[http://www.innosec.fi/miksi\\_suojautua/](http://www.innosec.fi/miksi_suojautua/)

Rousku, Kimmo 2003. Suunnitelmallisuus ohjaa toimintaa. MikroPC 4/2003, 54 - 56.

Supertroijalaiset tulevat 2006. MikroBitti 9/2006, 10.

Sähköisen viestinnän tietosuojalaki 16.6.2004/516. [Online] [Viitattu 14.3.2007].

<http://www.finlex.fi/fi/laki/ajantasa/2004/20040516>

Sähköisen viestinnän tietoturva ja –suoja 2006. [Online] [Viitattu 14.3.2007].

<http://www.ficora.fi/index/saadokset/lait/svt.html>

Tietotekniikkalaitteiden katoamisten ja varkauksien ehkäisy 2003. Suomen Vakuutusyhtiöiden Keskusliitto. [Online] [Viitattu 14.3.2007]

[http://www.innosec.fi/mp/db/file\\_library/x/IMG/30610/file/atklaitteet20031.pdf](http://www.innosec.fi/mp/db/file_library/x/IMG/30610/file/atklaitteet20031.pdf)

Tuotteet – Lukitus 2007. Innosec Oy. [Online] [Viitattu 12.3.2007]. <http://www.innosec.fi/tuotteet/lukitus/>

Turvamerkintä – EuroMark 2007. Innosec Oy. [Online] [Viitattu 12.3.2007].

<http://www.innosec.fi/tuotteet/turvamerkinta/euromark/>

Turvamerkintä – ID2S 2007. Innosec Oy. [Online] [Viitattu 12.3.2007]. <http://www.innosec.fi/tuotteet/turvamerkinta/id2s/>

Viestintävirasto 47 B/2004M - Määräys teleyritysten tietoturvasta 2004. [Online] [Viitattu 14.3.2007].

[http://www.ficora.fi/attachments/suomi\\_R\\_Y/1158858986420/Files/CurrentFile/Viestintavirasto47B2004M.pdf](http://www.ficora.fi/attachments/suomi_R_Y/1158858986420/Files/CurrentFile/Viestintavirasto47B2004M.pdf)

Viestintävirasto 48 B/2004M - Määräys viestintäverkon fyysisestä suojaamisesta 2004. [Online] [Viitattu 14.3.2007].



[http://www.ficora.fi/attachments/suomi\\_R\\_Y/1158858986686/Files/CurrentFile/Viestintavirasto48B2004M.pdf](http://www.ficora.fi/attachments/suomi_R_Y/1158858986686/Files/CurrentFile/Viestintavirasto48B2004M.pdf)

Wikipedia 2007. [Online] [Viitattu 15.3.2007]  
<http://fi.wikipedia.org/>

Wikipedia 2007. IMAP. [online] [viitattu 15.3.2007]  
<http://fi.wikipedia.org/wiki/IMAP>

Wikipedia 2007. POP3. [online] [viitattu 15.3.2007]  
<http://fi.wikipedia.org/wiki/POP3>

Wikipedia 2007. SMTP. [online] [viitattu 15.3.2007]  
<http://fi.wikipedia.org/wiki/SMTP>

## **Liitteet**

### ***Liite 1: PPCT Finland Oy – Tietoturvapoliittikka***

Hyväksytty PPCT Finland Oy:n ja *asiakasorganisaation* välisessä kokouksessa XX.XX.200X.

### **Tietoturvapoliittikka – PPCT Finland Oy & Asiakasorganisaatio**

Tietoturvapoliittikka on PPCT Finland Oy:n ja *asiakasorganisaation* johdon kannanotto, joka määrittelee organisaatioiden välisen ylläpitosopimuksen tietoturvallisuuden vastuut, tavoitteet ja toteutuskeinot.

Tietoturvallisuus nähdään osana PPCT Finland Oy:n toiminnan laatua.

### **Päämäärä ja tavoitteet**

Tietoturvallisuuden päämääränä on turvata *asiakasorganisaation* tietojärjestelmän keskeytyksetön toiminta ja estää sen oikeudeton käyttö. Lisäksi tavoitteena on estää *asiakasorganisaation* toiminnalle tärkeän tiedon tahaton tai tahallinen tuhoutuminen, vääristyminen ja väärinkäyttö. Tietoturvallisuudella pyritään varautumaan riskeihin ja minimoimaan niistä aiheutuvat vahingot.

Tietoliikennejärjestelmä, sen sisältämät tiedot ja järjestelmään kuuluvat laitteet pidetään suojattuina teknisten-, fyysisten- ja hallinnollisten toimenpiteiden avulla. Tietoturvallisuuden toteutumista tarkkaillaan jatkuvalla valvonnalla. Tietojärjestelmän suojausmenetelmät pidetään ajanmukaisina ja niitä kehitetään jatkuvasti vastaamaan hyvää kansainvälistä suojaustasoa.

Ennen kaikkea tietoturvallisuus nähdään osana *asiakasorganisaation* liiketoimintaa ja sen päämääränä on *asiakasorganisaation* liiketoiminnan jatkuvuuden turvaaminen.

### **Tietoturvallisuuden määritelmä**

*Tietoturvallisuudella* tarkoitetaan tietojenkäsittelyn turvaamista, jolla pyritään toteuttamaan luottamuksellisuuden, käytettävyyden, eheyden, kiistämättömyyden ja pääsynvalvonnan periaatteet. Tietoturvallisuus koskee kaikkia *asiakasorganisaation* tietojenkäsittelytehtäviä.

*Käytettävyys* tarkoittaa että tiedot ovat saatavissa oikeassa muodossa ja riittävän nopeasti.

*Eheys* tarkoittaa että tietojärjestelmän tiedot ovat luotettavia, eivätkä sisällä tahallisia tai tahattomia virheitä.

*Luottamuksellisuus* tarkoittaa että tiedot ovat vain oikeutettujen henkilöiden käytettävissä.

*Kiistämättömyys* merkitsee järjestelmän kykyä tunnistaa ja tallentaa luotettavasti käyttäjän tiedot. Kiistämättömyydellä tahdotaan varmistaa tiedon alkuperä ja tunnistaa niiden luvaton käyttö.

*Pääsynvalvonta* tarkoittaa niitä menetelmiä, joilla rajoitetaan tietojärjestelmän käyttöä.

*Tietoturvallisuustoimenpiteet* koskevat sähköisessä, kirjallisessa ja puhutussa muodossa olevan tiedon käsittelyä, luovutusta, arkistointia, siirtoa ja hävittämistä.

### **Vastuukysymykset**

Tietoturvallisuudesta ovat vastuussa PPCT Finland Oy ja *asiakasorganisaatio* yhdessä.

Ylin vastuu *asiakasorganisaation* tietoturvallisuudesta on *asiakasorganisaation* johdolla. Johdon sitoutuminen on tietoturvallisuuden toteutumisen lähtökohta. *Asiakasorganisaatio* vastaa hallinnollisesta turvallisuudesta, henkilöstö- ja toimitilaturvallisuudesta sekä tietojärjestelmälaitteiden fyysisestä turvallisuudesta. *Asiakasorganisaatio* on myös päävastuussa tietoineistonsa turvallisesta käsittelystä, säilyttämisestä ja hävittämisestä. Hallinnollinen seuranta sekä tarvittavan tietoturvallisuuskoulutuksen ja -ohjeistuksen järjestäminen ovat niin ikään *asiakasorganisaation* vastuualueita.

Vastuu tietoliikenneturvallisuuden teknisten ratkaisujen toteuttamisesta, ylläpidosta ja teknisestä valvonnasta on PPCT Finland Oy:llä. PPCT Finland Oy toteuttaa *asiakasorganisaation* tietoliikennejärjestelmän laitteisto- ja ohjelmistoasennukset, valvoo niiden toimintaa sekä suorittaa tarvittavat korjaus-, päivitys- ja huoltotoimenpiteet.

Viime kädessä jokainen *asiakasorganisaation* tietojärjestelmän käyttäjä on omalta osaltaan vastuussa tietoturvallisuudesta.

### **Osapuolten välinen salassapito**

Sopimuksen osapuolet sitoutuvat pitämään salassa kaiken organisaatioiden toimintaan liittyvän luottamuksellisen tiedon ja olemaan ilmaisematta niitä kolmannelle osapuolelle ilman toisen osapuolen kirjallista suostumusta. Salassapitovelvollisuus on voimassa myös ylläpitösopimuksen päättymisen tai irtisanomisen jälkeen.

Kumpikin osapuoli sitoutuu ilmoittamaan toiselle, mikäli tämän tiedot ovat vaarassa joutua tai ovat joutuneet väärinkäytön kohteeksi.

Mikäli tietojärjestelmän ylläpidossa tai toimittamisessa käytetään alihankkijoita, sen tulee tapahtua osapuolten yhteisen sopimuksen perusteella.

### **Lainsäädäntö**

Osapuolten toiminnassa huomioitavat ja molempia sitovat lainkohdat:

- Laki yksityisyyden suojasta työelämässä 13.8.2004/759
- Henkilötietolaki 22.4.1999/523
- Sähköisen viestinnän tietosuojalaki 16.6.2004/516, 4§ ja 6§

## Toteutuskeinot

Perustana tietoturvallisuuden toteuttamiselle on tämä kirjallinen tietoturvapoliittikka, joka annetaan tiedoksi *asiakasorganisaation* henkilöstölle sekä PPCT Finland Oy:n palveluksessa toimiville ylläpitäjille.

PPCT Finland Oy sitoutuu toteuttamaan ylläpitosopimuksen mukaiset tietoliikenneverkon tekniset ratkaisut ja niiden vaatimat suojauskeinot, sekä noudattamaan määriteltyjä tietoturvarutiineja. PPCT Finland Oy myös valvoo, ylläpitää ja huoltaa tietoliikennejärjestelmän toimintaa. Tekniset ratkaisut ja suojausmenetelmät kuvataan tarkemmin tietoliikenneverkon dokumentaatioissa. Tietojärjestelmän ylläpitoon liittyvät toimenpiteet kuvataan ylläpitudokumentissa.

*Asiakasorganisaatio* sitoutuu hallinnollisen-, fyysisen- ja henkilöstöturvallisuuden toteuttamiseen, sekä siihen liittyvään valvontaan ja ylläpitoon. *Asiakasorganisaatio* huolehtii tietoliikennejärjestelmänsä laitteiden suojaamisesta fyysisiltä uhilta, henkilöstön tietoturvakoulutuksen ja -ohjeistuksen järjestämisestä sekä henkilöstön tietoturvallisen toiminnan seurannasta. Lisäksi *asiakasorganisaatio* sitoutuu huolehtimaan tietoaineistonsa turvallisesta käsittelystä, luovuttamisesta, siirrosta, arkistoinnista ja hävittämisestä. Viime kädessä tiedon omistaja on vastuussa tietoturvaluustoimenpiteistä.

Tietoturvallisuutta ohjaavat ja tietoturvapoliittikkaa täsmentävät dokumentit pidetään vain asiномаisten henkilöiden saatavissa.

## Tiedottaminen

Tietoturvallisuuteen liittyvien asioiden tiedottamisesta PPCT Finland Oy:n ja *asiakkaan* välillä vastaavat PPCT Finland Oy:n ja *asiakasorganisaation* nimeämät vastuhenkilöt. Sopimuksen osapuolet vastaavat organisaationsa sisäisestä tiedottamisesta.

## Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely

PPCT Finland Oy suorittaa *asiakasorganisaation* tietojärjestelmän teknistä seuranta. Ongelmatilanteissa ylläpitäjä on velvollinen informoimaan *asiakasorganisaatiota* ja reagoimaan ongelman vaatimalla tavalla. Tarvittaessa ylläpitäjä voi myös suorittaa tietoturvallisuuden kartoituksia tietojärjestelmässä ja suosittaa toimenpiteitä havaittujen puutteiden tai vikojen korjaamiseksi. PPCT Finland Oy suorittaa toimenpiteet *asiakasorganisaation* suostumuksella.

Kriittisissä ja välitöntä reagointia vaativissa ongelmatilanteissa ylläpitäjä on oikeutettu ja velvoitettu suorittamaan korjaavat toimenpiteet välittömästi lisävahinkojen välttämiseksi. Ylläpitäjän suorittamat välittömät toimenpiteet saattavat aiheuttaa *asiakasorganisaatiolle* kuluja. Näin ollen PPCT Finland Oy ja *asiakasorganisaatio* sopivat välittömien toimenpiteiden vaatiman maksimisumman, jonka puitteissa ylläpitäjä voi suorittaa korjaavat toimenpiteet. Summan ylittyessä ylläpitäjä on velvollinen informoimaan *asiakasorganisaatiota* ja sopimaan jatkotoimenpiteistä yhdessä *asiakasorganisaation* edustajan kanssa.

*Asiakasorganisaatio* seuraa hallinnollisesti tietoturvallisuuden toteutumista organisaatioissa. Mikäli puutteita havaitaan, *asiakasorganisaatio* on oikeutettu ja velvoitettu suorittamaan kor-

jaavat toimenpiteet. *Asiakasorganisaation* on kuitenkin informoitava mahdollisista tietoturvallisuuden vaikuttavista muutoksista PPCT Finland Oy:tä. Mikäli muutokset vaativat toimenpiteitä ylläpitäjältä, PPCT Finland Oy on velvollinen suorittamaan tarvittavat toimenpiteet.

Jokainen tietojärjestelmän käyttäjä on velvollinen noudattamaan annettuja tietojärjestelmän sääntöjä ja ohjeita. Jokainen PPCT Finland Oy:n ylläpitäjä ja *asiakasorganisaation* tietojärjestelmän käyttäjä on myös velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, rikkomuksista tai väärinkäytöksistä PPCT Finland Oy:lle ja/tai *asiakasorganisaation* vastuuhenkilölle.

Tietoturvallisuuden rikkomukset tai väärinkäytöstapaukset johtavat tapauskohtaisesti hallinnollisiin tai oikeudellisiin sanktioihin.