Lasse Kivistö

# TIETOTURVASUUNNITELMA MIKROPASILLE

Tietojenkäsittelyn koulutusohjelma
Järjestelmäpalveluiden suuntautumisvaihtoehto
2011

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

# TIETOTURVASUUNNITELMA MIKROPASILLE

Kivistö, Lasse
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Huhtikuu 2011
Ohjaaja: Grönholm, Jukka
Sivumäärä: 42
Liitteitä: 1

Asiasanat: tietoturvasuunnitelma, tietoturvariski, tietoturva

---

Opinnäytetyöni aiheena on tietoturvasuunnitelma Mikropasi-nimiselle yritykselle. Vaikka opinnäytetyö on suunnattu Mikropasille, voi kuka tahansa lukija hyötyä lukemastaan. Opinnäytetyötä lukiessa huomaa kuinka vihamielinen Internet pahimmillaan voi olla. Tietoturvasuunnitelmassani olen perehtynyt tietoturvariskeihin, niiden ennaltaehkäisyyn ja toimenpiteisiin kun tietoturvariski realisoituu. Pääpainona on kuitenkin tietoturvariskien toteutumisen estäminen.

Tähän tietoturvasuunnitelmaan kuuluu hallinnollinen tietoturva, tietotekninen turvallisuus, fyysinen turvallisuus, tietoaineiston turvallisuus ja henkilöstön turvallisuus. Hallinnollinen tietoturva koostuu toimintaohjeista ja niiden seurannasta. Tietotekninen turvallisuus pitää sisällään tietoliikenteen, laitteet, ohjelmistot ja niiden käyttötavat. Fyysiseen turvallisuuteen kuuluu tavat suojata yrityksen tilat ja omaisuus varkaiden ja luonnonilmiöiden varalta. Keinot suojata yritykselle tärkeä tieto on tietoaineiston turvallisuutta. Henkilöstön turvallisuus pitää sisällään tahalliset tai tahattomat työntekijän aikaansaamat tietoturvariskit.

Tämä opinnäytetyö on suunniteltu ja toteutettu täyttämään kaikki tietoturvaan liittyvät nykypäivän vaatimukset. Opinnäytetyön toimeksiantajana ollut yritys voi nyt siis täydentää ja parantaa tietoturvaansa entisestään myös lähitulevaisuudessa.

INFORMATION SECURITY PLAN FOR MIKROPASI

Kivistö, Lasse
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information technology
April 2011
Supervisor: Grönholm, Jukka
Number of pages: 42
Appendices: 1

Keywords: information security plan, information security risk, information security

---

This thesis is about the information security plan for the company known as Mikropasi. Although the thesis has been directed to Mikropasi, any reader can benefit from what they have read. This thesis gives an idea to the reader how hostile Internet can be at its worst. In my thesis I have acquainted with the information security risks, how to prevent them happening and what to do when an information security risk comes reality. The focus, however, is on how to prevent the security risks happening.

This information security plan includes administrative security, technological security, physical security, data security and personnel security. Administrative security consists of operational guidelines and how to monitor them. Technological security includes telecommunications, hardware, software and how to use them. Physical security includes the ways to protect business premises and property from thieves and natural phenomena. Data security is the means how to protect important and valuable company information. Personnel security includes intentional or unintentional information security risks made by employees.

This thesis was designed and made so that it meets all the required demands in the present day information security. The company possesses now the knowledge how to improve their information security in the near future.

SISÄLLYS

# 1 JOHDANTO

Olin työharjoittelussa Mikropasissa viisi kuukautta, ja opin silloin jonkun verran uutta tietokoneista, niiden tietoturvasta ja komponenteista. Samalla pääsin tutustumaan yritykseen ja sen toimintaan lähietäisyydeltä. Pohtiessani opinnäytetyölle aihetta, melkein ensimmäisenä mieleen tuli Mikropasi. Seuraavaksi pohdin, että minkälaisen työn voisin sinne tehdä. Juteltuani muutamaan otteeseen Pasi Isomäen kanssa, syntyi ajatus tietoturvasuunnitelmasta. Minua kiinnostaa tietoturva, joten oli helppoa ryhtyä jatkotoimenpiteisiin.

Tietoturvalla tavoitellaan tiedon, järjestelmien ja palveluiden suojaamista kaikissa mahdollisissa olosuhteissa. Tietoturvasuunnitelma on suunnitelma miten näihin uhkiin varaudutaan ja miten toimitaan uhan toteutuessa. Mielestäni jokaisella yrityksellä, jolla on vähänkään Internetiin liittyvää toimintaa, pitäisi olla ajanmukainen ja aktiivinen tietoturvasuunnitelma.

Tässä tietoturvasuunnitelmassa on käsitelty seuraavanlaisia tietoturvaan liittyviä kokonaisuuksia ja osa-alueita: hallinnollinen tietoturva, tietotekninen turvallisuus, fyysinen turvallisuus, tietoaineiston turvallisuus ja henkilöstön turvallisuus. Mukaan on otettu kaikki tarpeellinen ja vähän ylikin, jotta Mikropasin tulevaisuuden näkymät ja mahdolliset tarpeet on tyydytetty mahdollisimman hyvin vastaamaan nykypäivän tietoturvauhkia vastaan.

# 2 TIETOTURVASUUNNITELMAN TARKOITUS

Internetin käyttö on lisääntynyt merkittävästi sen perustamisen jälkeen. Internet on tuonut paljon hyvää ja helpottanut monia asioita, mutta valitettavasti epärehellinen toiminta on myös lisääntynyt Internetin välityksellä enemmän ja enemmän. Esimerkiksi Suomessa oli vuosikymmen sitten vain kourallinen asiantuntijoita, jotka olisivat osanneet murtaa käyttöjärjestelmätason suojaukset. Nykyään lähes jokainen teini-

ikäinen pystyisi samaan. Tietotaito on lisääntynyt ja tiedon saatavuus on helpottunut. Työkalut järjestelmien murtoihin ovat halpoja, jopa ilmaisia.

Mikäli tietoturvassa on aukkoja, on todennäköistä, että jonkinlainen tietoturvaloukkaus tapahtuu ennemmin tai myöhemmin. Kaikki yrityksen tieto ei välttämättä ole arvokasta, mutta minkä tahansa tiedon joutuessa vääriin käsiin, voidaan sillä haavoittaa yrityksen luotettavuutta ja imagoa merkittävästi.

Tietoturvalla tavoitellaan yrityksen tiedon salassa pysymistä asiaankuulumattomilta henkilöiltä, tiedon helppoa saatavuutta ja sen oikeellisuutta. Tietoturvasuunnitelmaan sisältyy muutakin kuin vain tavat suojautua hakkereita ja haittaohjelmia vastaan. Tietoturvasuunnitelman tavoitteena on olla toimintaoppaana ja auttaa ennaltaehkäisemään erilaisia tietoturvaan liittyviä tilanteita.

# 3 TIETOTURVARISKIEN ANALYSOINTI

Kaikkiin tietoturvariskeihin ei voi, eikä kannata varautua. Kaikkien tietoturvariskien täydellinen välttäminen ei ole mahdollista. Ainoastaan riskeihin, jotka ovat todennäköisiä, ja joista realisoituessaan aiheutuu taloudellisia menoja, kannattaa varautua. (Tammisalo 2005, 9-10) Tosin esimerkiksi liiallinen rahallinen satsaus johonkin vanhaan laitteeseen, jonka arvo on lähes mitätön, ei ole järkevää (Cantrell, Lucas & Abhishek 2006, 8).


Kuva 1. Erilaisia tietoturvariskejä

**Jätehuolto**

Jätehuollon merkitystä ei pidä vähätellä. Roskissukellus eli roskisten penkominen on tehokas tapa löytää haluamansa tiedot. Tämän takia normaaleihin roskiksiin ei saa heittää yrityksen toimintaan liittyvää materiaalia, kuten IP–osoitteita, salasanoja, käyttäjätunnuksia ja niin edelleen. Papereiden silppuaminen ei auta, koska paperin pystyy kokoamaan uudelleen. (Kajala 2002, 75)

**Muistitikut**

Kannettavan laitteen sisältämä tieto on usein arvokkaampaa kuin laite itse (Laaksonen, Nevasalo & Tomula 2006, 168). On siis sanomattakin selvää, että pienikokoiset muistitikut on pidettävä varmassa tallessa, eikä niitä saa lojua ympäri yrityksen tiloja. Sama neuvo koskee myös muita kannettavia laitteita, joilla on yrityksen tai asiakkaiden tietoja.

**Ohjelmien haavoittuvuudet**

Ulkopuolinen henkilö kerää tietoa ohjelmien haavoittuvuuksien avulla. Tällä tarkoitetaan sitä, että kun hakkeri löytää ohjelmasta tietoturvareiän hän käyttää tätä apu-

naan uhrin tietojen keräämiseen esimerkiksi webselaimen avulla. Tämän takia on tärkeää päivittää ohjelmat kun niihin tulee päivityksiä. Ulkopuolinen henkilö voi myös väärentää websivuja ja tehdä niistä esimerkiksi verkkopankin sivujen kaltaisia ja tällä tavalla huijata käyttäjää antamaan verkkopankkitunnukset väärään tarkoitukseen.

**Phishing**

Phishing eli tietojen kalastelu on sähköpostitse tai puhelimitse tapahtuvaa hakkereiden urkintaa. Hakkeri tekeytyy esimerkiksi jonkin yrityksen tai pankin edustajaksi ja pyytää ilmoittamaan luottokorttitiedot, salasanan tai muita tunnuksia. Näitä apuna käyttäen hakkerilla on helppo työ viedä kohteensa rahat. (Jakobsson & Myers 2007, 1)

**Roskaposti**

Sähköpostin kautta leviävä roskaposti ei sisällä enää juurikaan haittaohjelmia, vaan roskapostinlähettäjät yrittävät myydä tuotteitaan. Roskapostia voi yrittää suodattaa, mutta jos sähköposti on kerran joutunut listalle, ei sitä sieltä pois saa koskaan. Paras tapa estää yrityksen tai oman sähköpostiosoitteen joutuminen postituslistalle on tehdä osoitteesta kuva ja sijoittaa se Internet-sivuille. Tällä tavoin roskapostinlähettäjien ohjelmat eivät osaa lukea sähköpostiosoitetta Internet-sivulta. Roskapostin suodatus auttaa karsimaan melko paljon roskapostia, mutta ei koskaan kaikkea. Jos suodatus on liian korkealla, on erittäin todennäköistä, että jotkin tärkeät viestit joutuvat myös suodatetuiksi. Sähköpostiviestien liitetiedostot on tarkistettava viruksien varalta ennen niiden avaamista.

**Uudet laitteet**

Vanhojen ja tuttujen laitteiden kanssa tietoturva saattaa olla hallussa. Uuden, vastahankitun laitteen kanssa tietoturva voi kuitenkin unohtua. Ulkopuolinen henkilö voi päästä helposti laitteeseen ja sen sisältämiin tietoihin käsiksi, mikäli tällä uudella laitteella on Internet-yhteys, esimerkkinä älypuhelimet. (Pulliainen & Suojanen 2011, 25)

**Webkamerat**

Käyttämättömät webkamerat muodostavat tietoturvariskin. Jos ulkopuolinen henkilö pääsee tietokoneeseen käsiksi, jossa on webkamera, voi hän ottaa kuvia, nauhoittaa videota ja myös jopa ääntä webkameran mikrofonin avulla. Tämän vuoksi kaikki käyttämättömät webkamerat tulisi poistaa käytöstä esimerkiksi olla asentamatta webkameran käyttöön tarvittavia ajureita.

## 3.1 Haittaohjelmat

Haittaohjelmia ovat esimerkiksi virukset, madot, troijalaiset ja mainosohjelmat. Haittaohjelmia on useanlaisia. Jotkin ovat hyvänlaatuisia ja toiset pahanlaatuisia. Ero hyvänlaatuisen ja pahanlaatuisen haittaohjelman välillä on se, että minkälaista vahinkoa kyseiset haittaohjelmat tekevät. Pahanlaatuisen haittaohjelman vaikutukset ovat nopeasti havaittavissa. Hyvänlaatuista haittaohjelmaa ei välttämättä edes havaita, mutta se kuitenkin aiheuttaa vahinkoa pitemmällä aikavälillä. Hyvänlaatuinen haittaohjelma ei ole vaaraton. (Kajala 2002, 348)

Tietokonevirus on ohjelma, joka tartuttaa muita ohjelmia monistaakseen itseään (Kajala 2002, 349). Tietokonemato on samankaltainen kuin tietokonevirus, mutta mato pysyy liikkeellä verkon kautta, toisin kuin virukset, jotka jäävät tiedostoihin ja ohjelmiin kiinni (Kajala 2002, 351). Troijalainen on vahinkoa aiheuttava haittaohjelma, joka on naamioitu joksikin muuksi ohjelmaksi, jonka käyttäjä haluaa asentaa. Asentamalla tämänlaisen ohjelman, troijalainen lähettää isännälleen esimerkiksi salasanoja ja tiedostoja. (Kajala 2002, 378) Mainosohjelma näyttää mainoksia Internetsivuilla, sähköpostissa tai muuten Internetiin liittyvissä palveluissa. Mainosohjelma voi pitää sisällään vakoiluohjelman, joka puolestaan voi esimerkiksi tallentaa näppäimistön painalluksia tai ottaa kuvia tietokoneen näytöstä. (Shelley & Vermaat, 426)

Haittaohjelmia vastaan tietokoneella pitää olla asennettuna viruksentorjuntaohjelmisto ja palomuuri. Palomuuri voi olla osana viruksentorjuntaohjelmistoa. Tietokone ei ole yhtään sen paremmin suojattu, jos sille on asennettuna useita eri viruksentorjun-

taohjelmistoja, vaan päinvastoin. Eri viruksentorjuntaohjelmistot voivat estää toistensa toiminnan.

## 3.2 Denial-of-Service

Denial-of-Service eli palvelunkieltohyökkäys kohdistuu www–palvelimen käyttöjärjestelmää vastaan. DoS–hyökkäys rajoittaa tai kokonaan estää www–palvelimen palveluiden käytön. Yleisimpiä palvelunkieltohyökkäyksiä ovat valtavien yhtäaikaisten verkkoyhteyksien muodostaminen samaan aikaan palvelimelle, ylimääräisten prosessien ajaminen palvelimen keskusmuistin tukkimiseksi tai palvelimen tiedostojärjestelmän lamaannuttaminen tarpeettomilla tai virheellisillä tiedostoilla. Kokonaan DoS–hyökkäyksen vaikutukselta ei pääse karkuun, mutta rajoittamalla tiettyjä www-palvelimen resursseja DoS–hyökkäystä voidaan lieventää. Lievennyskeinoja ovat käyttämättömien verkkoyhteyksien aikakatkaisu, palveluprosessien prioriteettien määrittely ja levytilanhallinta. Palvelimen kiintolevyn ylimääräiset kirjoitusoperaatiot tulisi poistaa ja systeemitiedostojen ja käyttäjähakemistojen eriyttäminen toisistaan esimerkiksi puolittamalla kiintolevy. (Toivonen 2002, 91)

## 3.3 Inhimilliset virheet

Työntekijöiden tekemiä tietoturvariskejä ovat:

- työtehtävien tekemättä jättäminen
- huolimaton tietojenkäsittely
- yrityssalaisuuden rikkominen
- viestittämiseen liittyvät huolimattomuudet
- sisäisten tietojen väärinkäyttö
- yksityisyydensuoja (Laaksonen, Nevasalo & Tomula 2006, 143)

Ihmiset tekevät virheitä. Näitä virheitä voidaan vähentää, jos työntekijät ovat saaneet tietoturvakoulutusta (Laaksonen, Nevasalo & Tomula 2006, 137). Yrityksen tietoturvallisuus perustuu osana henkilöiden kykyyn välttää turhia riskejä ja noudattaa tieto-

turvaohjeistusta. Omalla hyvällä esimerkillään voi vaikuttaa paljon muiden työntekijöiden suhtautumiseen tietoturvaan.

### 3.4 Henkilöturvallisuus

Työntekijöiden palkkaaminen ja työsuhteiden päättyminen ovat tietoturvariskejä (Laaksonen, Nevasalo & Tomula 2006, 138). Ennen kuin työntekijä palkataan tehtävään, on tarkistettava hänen taustojaan. Helpoin ja nopein tapa tehdä tämä on syöttämällä hänen nimensä Internetin hakukoneeseen. Internet on vain suuntaa-antava, joten paremman varmistuksen saa tarkistamalla ansioluettelon suosittelijoilta työnhakijan oikeellisuuden ja pyytämällä aikaisempien työpaikkojen työtodistukset. (Laaksonen, Nevasalo & Tomula 2006, 139) Uuden palkallisen työntekijän kanssa on laadittava salassapitosopimus.

Työsuhteen päättymiseen liittyy useita tietoturvariskejä. Yrityksen arvokasta tietoa, jota usein ei ole dokumentoitu, lähtee työntekijän mukana. Yrityksen maine voi vaarantua, jos irtisanomistilanteessa tapahtuva toiminta on puutteellista. Yrityksen esimiehen on arvioitava työntekijänsä käsittelemän tiedon kriittisyys, yrityksen omistamat immateriaalioikeudet ja seuraukset yritykselle, jos tiedot valuvat yrityksen ulkopuolelle. Yrityksen toiminta ei saa jumittua yhden työntekijän lähdön vuoksi. Sen takia on oltava tapa varmistaa pääsy työntekijän yrityksen kannalta tärkeisiin tietoihin, jos työntekijä ei ole yhteistyöhalukas. (Laaksonen, Nevasalo & Tomula 2006, 144)

## 4 FYYSINEN YMPÄRISTÖ

Fyysinen ympäristö sisältää organisaation tuotanto- ja toimitilat. Lisäksi näissä tiloissa olevat tietojenkäsittelylaitteet kuuluvat fyysiseen ympäristöön (Tammisalo 2005, 43). Fyysistä ympäristöä pyritään suojaamaan seuraavilta tietoturvariskeiltä: palo- ja vesivahingot, ilkivalta, varkaus, sähkökatko ja pöly (Laaksonen, Nevasalo & Tomula 2006, 126) Koskaan ei voi olla liian hyvin suojattu ja koko ajan on todennäköisem-

pää, että jotain tapahtuu. ”Tietojenkäsittely on suunniteltava ja toteutettava siten, että tietojen saatavuus, oikeellisuus, luottamuksellisuus ja käytön seurattavuus eivät vaarannu.” (Tammisalo 2005, 11)

## 4.1 Fyysisten tietoturvariskien minimointi

Fyysisten tietoturvariskien minimointiin sisältyy yrityksen toimitilojen fyysinen suojaus. Fyysisellä suojauksella pyritään ennaltaehkäisemään yrityksen tietojen tuhoutuminen, vahingoittuminen tai tietoihin luvaton pääsy. (Laaksonen, Nevasalo & Tomula 2006, 126) Yritys myy erilaisia käyttötavaroita ja laitteita liiketilassaan. Tietokoneiden huolto toimii myös samassa tilassa. Asiakkailla on siis mahdollisuus nähdä ja koskea lähes kaikkea yrityksen liiketilassa. Tämän vuoksi asiakkaiden huollossa olevien tietokoneiden turvallisuus ja yksityisyys on turvattava. Yksi tapa olisi eritellä huolto- ja liiketilat toisistaan. Laitetilassa on huolehdittava, että laitteilla on riittävä ilmastointi. Ilmastointi ehkäisee laitteiden ylikuumenemisen.

Hälytysjärjestelmät ovat poissa päältä keskellä päivää. Päiväsaikaan tapahtuvat varkaudet ovatkin yleistyneet. Tämän vuoksi kamera- ja kulunvalvonta on erittäin suositeltava ominaisuus keskellä päivää, aivan kuin se on yölläkin. (Laaksonen, Nevasalo & Tomula 2006, 126) Laitteen sisältämä tieto on usein arvokkaampaa kuin laitteen arvo (Laaksonen, Nevasalo & Tomula 2006, 168). Virustorjunta, palomuuri ja päivitykset on oltava kunnossa ja päivitettyinä laitteen ollessa Internetissä. Tällöin estetään mahdolliset tietomurrot ja tietovarkaudet.

### 4.1.1 Hälyttimet ja valvontalaitteet

Valvontalaitteita tulee olla tiloissa, joissa yrityksen laitteet sijaitsevat. Valvontalaitteita ovat liikkeenilmaisimet, keskuslaite ja hälyttimet, jotka ilmoittavat vartiointiliikkeeseen liikkumisesta luvattomalla alueella. Laitetiloihin luovutettavista avaimista tulisi laatia lista, jossa pidetään kirjaa kenellä avaimet ovat ja koska ne on palautettu. Esimerkiksi työsuhteen päättymisen myötä palauttamattomat avaimet ovat tietoturvariski. (Laaksonen, Nevasalo & Tomula 2006, 126)

Lain mukaan kulunvalvonta on lievempi kuin kameravalvonta. Turvallisuuden määrää lisää kameravalvonta osana kulunvalvontaa. Nykypäivänä kannattavin tapa nauhoittaa turvakameroiden kuvaa on digitaalinen muoto. Digitaalisen muodon puolesta puhuu käytännöllisyys ja kuvanlaatu. Mahdolliset kameralaitteet tulisi sijoittaa siten, että ne edesauttavat turvallisuutta. Esimerkki hyvästä paikasta on sisäänkäynnit. Kamerat eivät saa osoittaa kohti työntekijöiden toimipisteitä. (Laaksonen, Nevasalo & Tomula 2006, 51-53)

## 4.2 Muut fyysisen ympäristön riskit

**Tulipalo**

Laitetila on oltava erillään muusta tilasta. Tulipalon sattuessa laitetilaan ei näin pääse savua, joka voisi vahingoittaa laitteistoa. Lämpötilan vaihtelua tulee tarkkailla erilaisilla antureilla, jotka mittaavat lämpöä ja ilmoittavat ennalta määritellyn lämpötilan ylittymisen. Laitetilassa on oltava riittävä ilmastointi, jotta laitteet pysyvät sopivien lämpötilojen sisällä. Mahdolliset tulevat laitehankinnat pitää ottaa huomioon laitetilassa ilmastoinnin kannalta. (Laaksonen, Nevasalo & Tomula 2006, 127) Palohälyttimet on oltava toiminnassa.

**Vesivahinko**

Vesivahingon välttämiseksi laitetilassa tai sen yläpuolella ei tulisi olla vesiputkia. Mikäli yläpuolella on vesiputkia, hyvä keino välttää vesivahinko on rakentaa välipohja. (Laaksonen, Nevasalo & Tomula 2006, 127) Laitteita ei kannata pitää lattialla, vaan siirtää pöydälle tai jotenkin muuten nostaa irti lattiasta tukevan tason päälle.

**Sähkökatko**

Sähkökatkot ja sähköhäiriöt voivat rikkoa laitteita aiheuttaessaan käyttökatkoja. Ylijännitesuoja vähentää sähköhäiriön riskiä verkkovirran virtapiikeiltä, esimerkiksi ukkoselta. Sähkökatkoihin voi varautua UPS-laitteilla tai varageneraattoreilla. Nämä laitteet on testattava säännöllisesti. (Laaksonen, Nevasalo & Tomula 2006, 127)

**Pöly**

Pölyn määrää voidaan vähentää säännöllisellä siivouksella ja laitetilan käytön rajoittamisella. Laitetila ei tulisi olla varastona, eikä työskentelypisteenä. Vesi- ja pölyvahinkojen estämiseksi laitteisto kannattaa nostaa lattiatasosta korkeammalle. (Laaksonen, Nevasalo & Tomula 2006, 127)

# 5 PALVELIMET JA TYÖASEMAT

## 5.1 Palvelimet

Ohjelmistot on oltava ajan tasalla. Palvelimet on päivitettävä mahdollisimman nopeasti, kun siihen on mahdollisuus. Palvelimia ja niiden ohjelmistojen päivittämistä ja seurantaa helpottaa laiterekisteri (Laaksonen, Nevasalo & Tomula 2006, 156). Turhat palvelut tulee karsia pois palvelimilta. Varsinkin verkkopalveluiden kanssa pitää olla tarkkana, ettei palvelimille ole tietämättä asennettuna takaporttia hakkerille. (Toivonen 2002, 45)

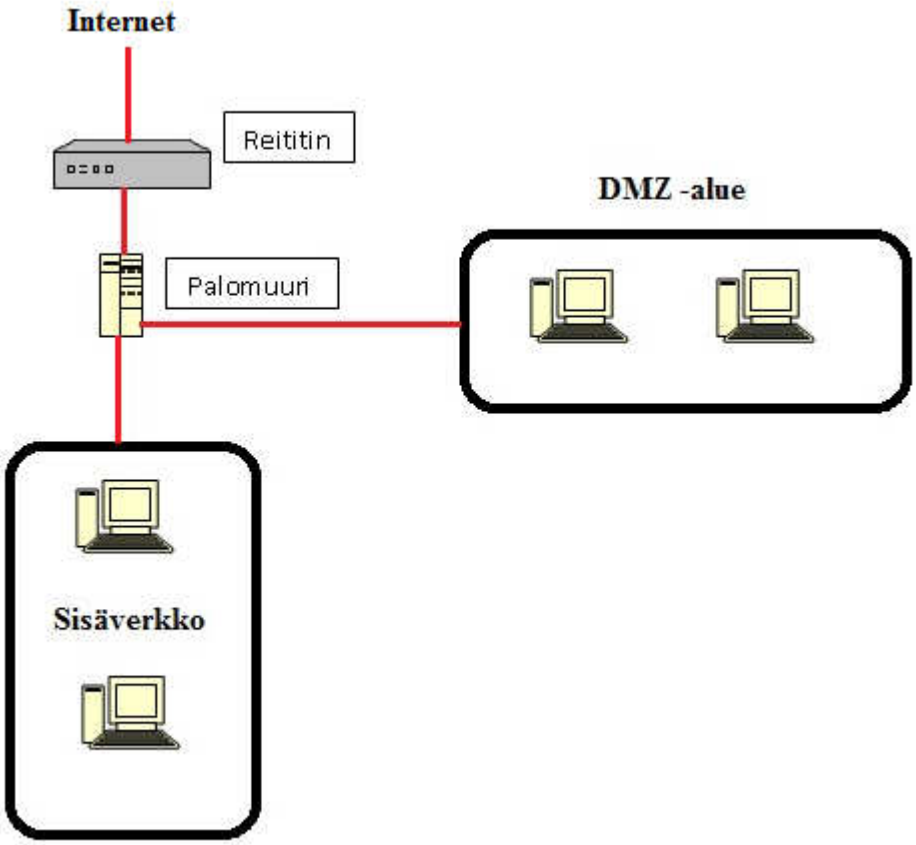
Palvelimet tulisi luokitella niiden tärkeysasteiden mukaan. Luokittelussa tulisi käyttää enintään neljää tärkeysluokkaa. Kolme tärkeysluokkaa on tarpeeksi Mikropasin tämän hetkisessä tilanteessa. Tärkeysluokat ovat taulukossa 1. Palvelimien käytettävyys ja niiden sisältämien tietojen kriittisyys ovat tärkeimmät määrittelytavat palvelimien tärkeysluokittelussa. (Laaksonen, Nevasalo & Tomula 2006, 158-159)

Taulukko 1. Palvelimien tärkeysasteiden luokittelu

| **Tärkeysaste**<br>**Määrite** | **Kriittinen** | **Tärkeä** | **Ei-tärkeä** |
|---|---|---|---|
| Palvelimen ominaisuus | Ilman tätä palvelinta yrityksen toiminta keskeytyy | Tämä palvelin on keskeisenä osana yrityksen toimintaa. Toiminta voi kuitenkin jatkua hetkellisesti ilman tätä palvelinta | Palvelin, joka ei vaikuta lähes ollenkaan yrityksen päivittäiseen toimintaan |
| Palvelimen keskeytyksen enimmäisaika | Enintään 5 minuuttia | 3 – 5 tuntia | Useita päiviä |
| Palvelimessa olevan tiedon kriittisyys | Kaikkien mahdollisten olosuhteiden vaikutuksien alla tietojen säilyminen ja saatavuus on turvattava | Ainoa ero kriittiseen palvelimeen on tietojen saatavuuden aikaviive, joka on maksimissaan 3 – 5 tuntia | Tietojen säilyminen ja saatavuus olisi turvattava, vaikka tietojen menetys ei ole yrityksen kannalta merkittävää |
| Identtisen vara-palvelimen pakollisuus | Pakollinen | Suositeltava | Ei tarpeellinen |

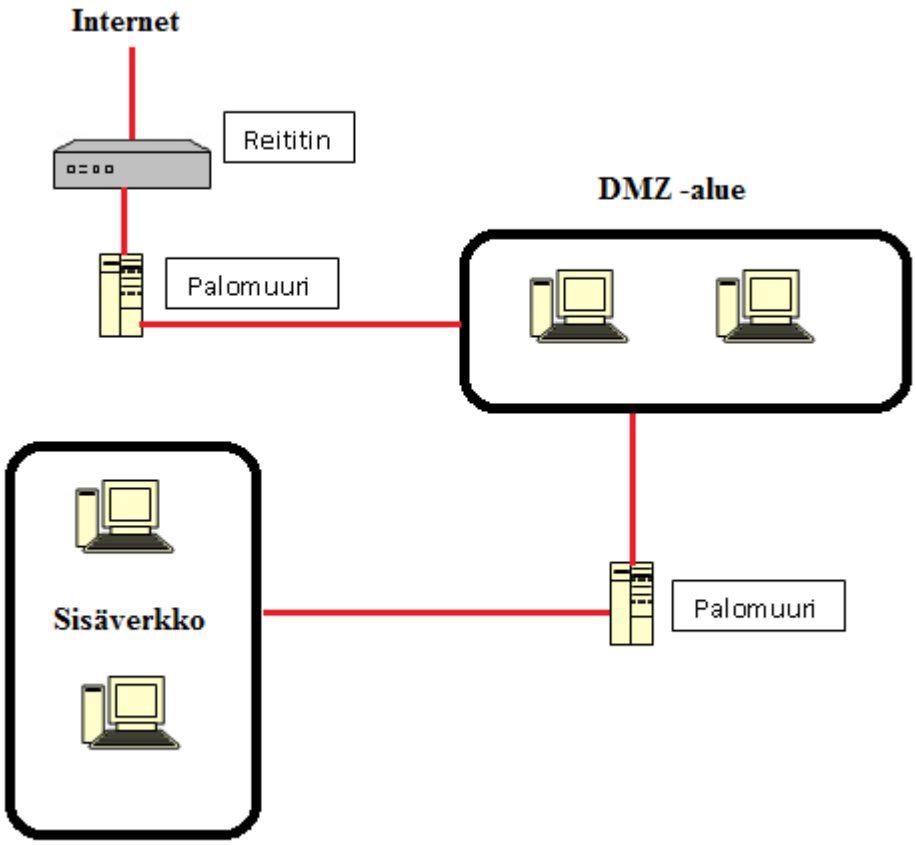
### 5.1.1 DMZ

Demilitarisoitua aluetta käytetään fyysisenä tai loogisena aliverkkona lisäämään tietoturvaa yrityksen palvelimien ja Internetin välillä. On olemassa monenlaisia DMZ–ratkaisuita. DMZ–palvelimet eivät ole palvelimia, joissa on yrityksen tärkeitä tietoja, vaan palvelimia, jotka hallinnoivat vain lähinnä verkkoliikennettä. Yrityksen palvelimet, jotka sisältävät yrityksen tärkeimmät tiedot sijaitsevat sisäverkossa, joka on erillään DMZ–palvelimista. Yksinkertaisin DMZ–ratkaisu lienee yhden palomuurin takana olevat webpalvelut, kuten www-, sähköposti- ja DNS–palvelimet. Nämä palvelimet ovat irti yrityksen sisäisestä verkosta omana verkkonaan, kuten kuvasta 2 käy ilmi. (Cantrell, Lucas & Abhishek 2006, 29-35)




Kuva 2. Yhden palomuurin DMZ–ratkaisu

Kuvassa 3 on esiteltynä kahden palomuurin ratkaisu, joka on turvallisempi ratkaisu kuin yhden palomuurin ratkaisu. Tällöin yrityksen ulkoa tulevaa verkkoliikennettä hallinnoi ulkoinen palomuuri, jonka kautta tietoliikenne on sallittu menemään vain DMZ–palvelimiin. Sisäverkkoon tietoliikenne kulkee sisäisen palomuurin kautta DMZ–palvelimilta. (Cantrell, Lucas & Abhishek 2006, 29-35)



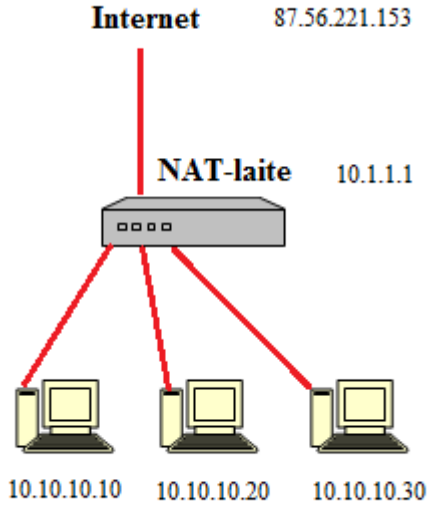

Kuva 3. Kahden palomuurin DMZ–ratkaisu

Yhden palomuurin ratkaisutapaa puoltavat sen edullisuus, helppo muodostus ja vähäinen ylläpito. Yhden palomuurin ratkaisutapa ei sovellu kasvavan yrityksen ratkaisuksi ja tietoturvallisuudeltaan yksi palomuuri on heikompi kuin kaksi palomuuria. Hyviä puolia kahden palomuurin käyttöratkaisussa on sen monipuolisuus erilaisine palvelimien sijoitusmahdollisuuksineen ja sen tietoturvallisuuden taso. Heikkouksina on, että se maksaa enemmän kuin yhden palomuurin käyttöratkaisu ja kahden palomuurin tarkkailuun kuluu huomattavasti enemmän aikaa ja resursseja. (Cantrell, Lucas & Abhishek 2006, 37-38)

### 5.1.2 NAT

NAT eli network address translation yleistyi yritysten käytössä, koska IP–osoitteet alkoivat vähentyä. Nykyisin osoitteenmuunnosta käytetään IP–osoitteiden piilottamiseen. Osoitteenmuunnoksen tekevä laite, joka on palomuuri tai reititin, muuttaa sisäisen IP–osoitteen julkiseksi. Useat eri laitteet voivat siis käyttää samaa ulkoista IP–

osoitetta liikennöidessään Internetissä. (Beekelaar, Komar & Wettern 2003, 62) NATista on olemassa kaksi erilaista versiota. Staattinen NAT tarvitsee pysyvän julkisen IP–osoitteen jokaiselle isäntä-koneelle sisäisessä verkossa. Dynaaminen NAT antaa automaattisesti julkiset osoitteet tarvittaessa. Kun IPv6 on yleistynyt nykyisen IPv4n tilalle, NATille ei ole enää tarvetta. (Leiden, Wilensky & Bradner 2009, 83) Kuvassa 4 on esiteltynä miten IP–osoitteet voidaan vaihtaa NATin avulla. Ylin IP–osoite on se, joka näkyy Internetiin. Muut osoitteet ovat sisäisiä.




Kuva 4. Esimerkki osoitteenmuunnoksesta

Hakkerin on vaikeampaa päästä NATin takana oleviin tietokoneisiin, koska yksityiset verkko-osoitteet eivät välity Internetiin operaattoreilta. Mikäli operaattorit eivät jostain syystä estä yksityisten verkko-osoitteiden välittymistä Internetiin, ei ole mahdollisuuksia tietää mille lukemattomista Internetissä olevista tietokoneista tämä IP–osoite kuuluu. NAT ei kuitenkaan pysty suojaamaan tietokonetta käyttäjän tekemiltä virheiltä, kuten käyttäjän muodostamaa yhteyttä vihamieliselle tietokoneelle. (Beekelaar, Komar & Wettern 2003, 63-64)

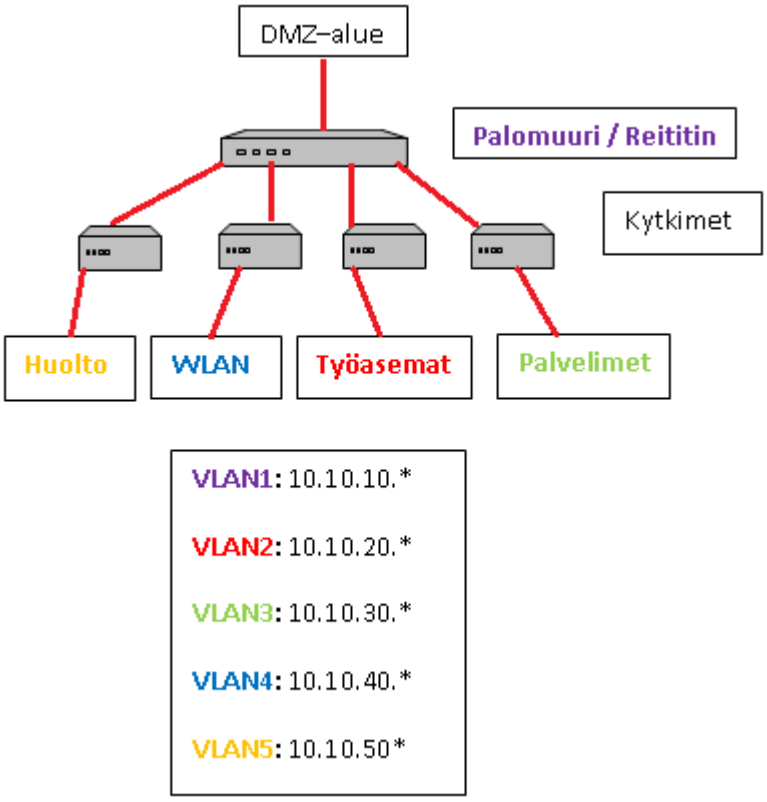
Yksityiset IP–osoiteavaruudet:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Nämä IP–osoitteet ovat varattuja yksityiseen käyttöön, eikä niitä käytetä Internetissä. (Beekelaar, Komar & Wettern 2003, 63)

### 5.1.3 VLAN

VLAN eli virtuaalinen lähiverkko mahdollistaa fyysisen lähiverkon jakamisen useisiin virtuaalisiin lähiverkkoihin. Jokainen VLAN saa oman ainutlaatuisen numeronsa, joka toimii tunnuksena fyysisessä lähiverkossa. Eri VLANit jakavat lähiverkon kytkimet ja muut laitteet, mutta jokainen VLAN toimii loogisesti itsekseen. (Feit 2000, 307) Virtuaalinen lähiverkko soveltuu erilaisiin tarkoituksiin. VLAN voi olla pysyvä ratkaisu tai hetkellinen. Eri VLANit voidaan määritellä eri tarkoituksiin ja ne voivat pitää sisällään esimerkiksi yrityksen työasemat, palvelimet, langattoman lähiverkon tai asiakkaiden huollossa olevien tietokoneiden työpisteen. (Feit 2000, 308) Kuvassa 5 on yhdenlainen esimerkki virtuaalisten lähiverkkojen käyttömahdollisuudesta. Jokaisella VLAN:lla on oma kytkimensä, joka jakaa virtuaalista lähiverkkoa niin monelle laitteelle kuin on tarve. Jokaisella kytkimellä on oma IP–osoiteavaruus.




Kuva 5. Esimerkki useiden virtuaalisten lähiverkkojen käytöstä

VLANiin liittyviä hyötyjä ovat verkkoliikenteen vähentyminen ja tehokkaampi käyttö, parempi tietoturva ja yrityksen tietoverkon helpompi hallittavuus ja joustavuus. VLANin sisällä olevat tietokoneet lähettävät tietoja vain toisilleen oman lähiverkon sisällä, eivätkä rasita muuta yrityksen verkkoa. Tietoturva paranee VLANin avulla, koska VLANista ei pääse toiseen VLANiin, jos kytkimen portit on määritelty oikein. Kytkimen portit voidaan määritellä kiinteästi tiettyyn VLANiin. Tällä tavalla estetään pääsy VLANista toiseen IP–numeroa vaihtamalla. Hallittavuus ja joustavuus ovat helpompia, koska jokaisen VLANin hallinta tapahtuu yhdestä paikasta. (Angelescu 2010, 418) Virtuaaliset lähiverkot on hyvä merkitä erivärisinä verkkokaapeleina lisäämään hallittavuutta.

### 5.1.4 RAID

Useat erilaiset RAID–ratkaisut auttavat tietokonetta, joko vikasietoisuudessa tai nopeudessa, jolloin kokonaissuoritustaso nousee. Tietokoneen toimintavarmuus kuitenkin laskee sitä mukaa, mitä enemmän kiintolevyjä RAID–toteutuksessa on. Yhdessä RAID–ratkaisussa on aina enemmän kuin yksi kiintolevy. (Singh 2009, 108) Yksi RAID–ratkaisu toimii paremmin yhdessä palvelimessa, ja toinen RAID toimii paremmin toisessa.

**RAID 0**

RAID 0 on edullisin vaihtoehto. Tätä ratkaisua käytetään kun halutaan yhdistää monta erillistä kiintolevyä yhdeksi suureksi kokonaisuudeksi. RAID 0 käyttää ratkaisuista ainoana kaikkien kiintolevyjen kapasiteetit kokonaisuudessaan. RAID 0n heikkous on, että sillä ei ole yhtään vikasietoisuutta. Kaikki tieto menetetään, jos yksikin kiintolevy hajoaa. Vahvuutena on paras mahdollinen suoritustaso. Paras käyttökohde tälle ratkaisulle ovat korkeaa suorituskykyä vaativat sovellukset, jotka eivät ole kriittisiä yrityksen toiminnan kannalta. (Singh 2009, 112)

**RAID 1**

RAID 1 peilaa eli kirjoittaa saman tiedon jokaiselle kiintolevylle. Tämän takia RAID 1 on ratkaisuista kallein, koska kiintolevyjen yhteiskapasiteetista on käytössä vain puolet. Hyvää tässä ratkaisussa on, että tietoa ei menetetä, jos yksi kiintolevyistä rik-

koutuu. Vikasietoisuutta vaativissa järjestelmissä RAID 1 on erittäin käyttökelpoinen ratkaisu. (Singh 2009, 112)

**RAID 0+1**

RAID 0+1 käyttää hyväkseen RAID 0- ja RAID 1 -ratkaisuita yhdistäen näiden parhaat ominaisuudet. RAID 0+1 tarvitsee toimiakseen vähintään neljä kiintolevyä, joista ensimmäisellä parilla on tallennettu tieto ja toinen pari peilaa tallennetun tiedon. Ratkaisuna RAID 0+1 on kallis, mutta sen erinomainen suorituskyky ja hyvä vikasietoisuus puoltavat sen puolesta.

**RAID 5**

RAID 5 tarvitsee toimiakseen vähintään kolme kiintolevyä, joista yhden kiintolevyn kapasiteetti menetetään. Ylimääräistä kiintolevyä hyödynnetään tuomaan vikasietoisuutta käyttämällä pariteettidataa kiintolevyjen kesken. Tieto kiintolevyillä menetetään vain jos kiintolevyistä hajoaa enemmän kuin yksi. RAID 5 sopii hyvin yleisratkaisuna kaikkiin palvelimiin. (Singh 2009, 113)

### 5.1.5 Palvelimien liitännät

Yrityksen palvelimista olisi hyvä poistaa kaikki turhat liitännät, kuten USB–liitännät ja infrapuna-, WLAN- ja Bluetooth–yhteydet. Tällä tavalla yrityksen tieto ei leviä helposti esimerkiksi käyttäjän muistitikulle. Työasemissa vastaava tilanne voidaan välttää asentamalla erillinen sovellus estämään PED–laitteiden käyttö. (Laaksonen, Nevasalo & Tomula 2006, 222)

## 5.2 Työasemat

Kaikki Mikropasin omistamat ja työntekijöiden käytössä olevat tietokoneet ja laitteet on tarkoitettu vain työtehtävien hoitoon. Käyttämättömässä työasemassa pitää olla salasanalukitus, kun työasema on ollut käyttämättömänä määrätyn ajan. Tietokoneen käyttäjä ei aina kuitenkaan muista lukita tietokonetta ennen poistumistaan sen luota. Työasemien monitorien ruudut saavat olla näkyvissä vain työntekijöille.

### 5.2.1 Ohjelmat ja lisenssit

Työasemista pitää poistaa kaikki turhat ohjelmat ja palvelut, esimerkiksi tiedostojen jako. Turhat palvelut voivat toimia takaporttina, jota käyttämällä luvaton henkilö voi päästä yrityksen verkkoon. (Toivonen 2002, 46) Mikropasin omistamiin tietokoneisiin saa asentaa vain niitä ohjelmia, joihin yrityksellä on hallussaan lisenssi. Jos käyttäjä tarvitsee jonkun ohjelmiston käyttöönsä, tulee hänen pyytää lupa vastuuhenkilöltä. Ohjelmien lisenssit tulisi olla kirjattuna yhteen yhtenäiseen rekisteriin. Tällä tavalla tiedetään yrityksen koneissa olevat ohjelmat, eikä jo olemassa oleviin ohjelmiin tarvitse ostaa uutta lisenssiä uudestaan. Rekisteriä on pidettävä ajan tasalla ja päivitettävä kun uusia ohjelmia asennetaan. Säännöllinen ohjelmien inventointi on suotavaa, koska se auttaa pitämään rekisteriä ajan tasalla ja samalla turhat ja vanhentuneet ohjelmistot voidaan poistaa. (Laaksonen, Nevasalo & Tomula 2006, 153)

Työntekijä ei saa missään tapauksessa asentaa itse hankittuja tai Internetistä ladattuja ohjelmia yrityksen tietokoneille, vaikka ohjelma olisikin ilmainen ja sen tarkoitus on hyvämielinen. Ilmainen, Internetistä ladattu ohjelma voi tuoda haittaohjelman mukanaan. Kyseinen haittaohjelma voi esimerkiksi kerätä tietoa käyttäjän toimista ja salasanoista, ja lähettää ne eteenpäin ohjelman tekijälle.

### 5.2.2 Internetin käyttö

Vierailu sivustoilla, joista on todennäköistä saada haittaohjelmia työasemalle, tulisi estää ja suodattaa ohjelmallisesti. Tällaisia sivustoja ovat mm. aikuisviihde. Tiedostojen luvaton jakaminen ja niiden hallussapito on laissa kielletty. Internetin vähäistä käyttöä työntekijän omiin yksityisten asioiden hoitoon ei tulisi kieltää. (Laaksonen, Nevasalo & Tomula 2006, 164-165)

Sähköpostin käyttöön voidaan soveltaa samoja asioita kuin on edellä mainittu. Sähköpostiosoite, joka on yhteiskäytössä, vähentää sähköpostiin liittyviä ongelmia. Yrityksen yhteiskäytössä oleva sähköpostiosoite voisi olla myynti@yritys.fi tai asiakaspalvelu@yritys.fi. Erityishuomioita sähköpostiin liittyen ovat:

- tapa, jolla sähköpostiosoite julkaistaan ja esitetään yrityksen Internet-sivuilla

- työntekijän poissaoleminen ja työsuhteen päättyminen
- henkilökohtaiset sähköpostiviestit
- väärään osoitteeseen saapuneet viestit
- lähetetyt, mutta vastaanottamattomat viestit
- sen salaus, liitetiedostot ja roskaposti (Laaksonen, Nevasalo & Tomula 2006, 165-166)

Facebookin tai minkään muunkaan samanlaisen palveluntarjoajan tilapäivityksissä ei saa olla mitään, mikä viittaa yrityksen sisäisiin asioihin. Tämän kaltaisia asioita ovat esimerkiksi ennalta määritellyt poissaolot, ongelmat yrityksen järjestelmissä ja niin edelleen. Kenenkään tuntemattoman henkilön lähettämiä pikaviesteissä tai esimerkiksi Facebookin viesteissä olevia Internet-linkkejä ei saa avata (Pulliainen 2011, 25).

### 5.2.3 Virtualisointi

Virtualisoinnilla voidaan tarkoittaa montaa eri asiaa, mutta tässä työssä keskitytään vain tapaan mahdollistaa usean eri käyttöjärjestelmän suorittaminen yhdellä fyysisellä tietokoneella. Fyysisellä tietokoneella pitää olla tarvittavat resurssit, jotta se pystyisi suorittamaan virtuaalikoneita. (Carswell & Webb 2009, 2) Virtualisointi tarvitsee toimiakseen virtualisointiin tarkoitetun ohjelman, kuten VMware. Virtualisoinnin etuja ovat tietokoneen käyttämättömien resurssien hyödyntäminen, uuden tietokoneen nopea käyttöönotto ja virtuaalikoneen joustava ylläpito (Carswell & Webb 2009, 5).

Heikkouksia virtualisoinnissa ovat virtuaalikoneiden suorituskyky ja rajoittuvuudet isäntäkoneen resurssien mukaan. Virtuaalikoneita voidaan käyttää esimerkiksi uusien järjestelmien ja sovelluksien testaamiseen, käyttäjille tuntemattomien käyttöjärjestelmien tai sovelluksien opettamiseen ja esittelyyn. (Carswell & Webb 2009, 6) Virtualisointi edistää tietoturvaa, koska yrityksen työasemat voivat olla massamuistittomia, lähiverkon kautta toimivia päätelaitteita. Virtuaalikoneessa tapahtuvat virheet eivät vaikuta muihin virtuaalikoneisiin. Eri palvelut voidaan jakaa useille eri virtuaalikoneille, eivätkä ulkopuoliset henkilöt pääse näin käsiksi toisella virtuaalikoneella

oleviin tietoihin. Virtualisointi on edullinen ratkaisu, koska ei tarvita monia fyysisiä tietokoneita kuluttamassa sähköä, eikä uusille kalliille komponenteille ole samanlaista tarvetta kuin, jos olisi useampi fyysinen tietokone. (Blokdijk & Menken 2008, 35-37) Virtualisointia voidaan käyttää hyödyksi myös palvelimissa.

# 6 PALOMUURI JA REITITIN

## 6.1 Palomuuri

Palomuurilla estetään ulkopuolisia pääsemästä yrityksen verkkoon (Kajala 2002, 200). Palomuureja on monenlaisia, kuten omaa käyttöjärjestelmää käyttäviä ja erityisesti palomuureja varten räätälöityjä tutumpia käyttöjärjestelmiä, kuten Linux ja Windows (Andrés & Kenyon 2004, 434). Palomuuri on usein enemmän kuin vain pelkkä palomuuri. Tärkeitä palomuurin ominaisuuksia ovat: hallittavuus, liikennemäärän riittävä käsittely, salatun liikenteen tarkistaminen, lokitietojen keskitys ja sovelluksien käyttämän liikenteen tarkistaminen (Laaksonen, Nevasalo & Tomula 2006, 188). Muita palomuurin ominaisuuksia ovat: sisällön suodatus, VPN, NAT, kuorman tasaus ja vikasietoisuus. Sisällön suodatus auttaa estämään yrityksen verkossa olevia käyttäjiä pääsemästä tietynlaisille Internet-sivustoille. Kuorman tasaus jakaa ja hajauttaa verkkoliikennettä. Vikasietoisuus mahdollistaa palomuurin peilaamisen toiseen palomuuriin, jolloin toinen laitteista on käyttövalmiina, jos toiseen laitteeseen tulee vika. (Kajala 2002, 202) Tietoliikenne verkossa vaikeutuu, jos suojaukset on asetettu liian tiukoiksi. Turvallisempi ympäristö tarkoittaa heikompaa toiminnallisuutta. (Kajala 2002, 209)

Palomuurin läpi kulkevaa verkkoliikennettä voidaan tarkkailla IDSn avulla. IDS eli intrusion detection system ei auta millään muulla tavalla kuin vain antamalla hälytyksen, kun se havaitsee normaalista poikkeavaa toimintaa verkossa. IDS säädetään toimimaan yhdessä palomuurin kanssa. (Kajala 2002, 245-246) Lokeja tarvitaan esimerkiksi vianhaussa, verkkovikojen paikallistamisessa ja tunkeutujien jälkien seuraamisessa (Kajala 2002, 258). Varmin tapa estää lokien muokkaamista on kirjoittaa lokit yksisuuntaiselle laitteelle, joka tallentaa lokit kerran kirjoitettavalle tallenteelle

tai käyttämällä suojattua, vain lokeille tarkoitettua palvelinta. Yleisin käytössä oleva lokien keräysprotokolla on syslog, joka on integroituna useimpiin palomuureihin. (Kajala 2002, 259) Lokit ovat todistusaineistoa kun hakkeria syytetään verkkoon tunkeutumisesta (Kajala 2002, 269).

### 6.1.1 Vahvuudet ja heikkoudet

Erilaisilla palomuureilla on omat vahvuudet ja heikkoudet. Uutta palomuuria hankkiessa on hyvä perehtyä eroavaisuuksiin paremmin. Palomuuri ei vastaa yksinään suojauksesta, vaan se on vain osa suojausta. Ei pidä luottaa liikaa palomuurin toimintaan, vaan pitää myös pitää huolta sisäisten verkkojen tietoturvasta. (Kajala 2002, 210) Joitakin palomuureja on helpompi räätälöidä omaan tarkoitukseen kuin toisia. Palomuurien päivitysmahdollisuudet vaihtelevat. Jotkin palomuurit ovat käyttöominaisuuksiltaan monipuolisia ja helpompia ylläpitää kuin toiset. Palomuurien sisäinen tallennustila vaihtelee, mutta lokien säilytystä varten on olemassa muitakin mahdollisuuksia. Palomuurien suorituskyvyssä on eroavaisuuksia. Jotkin palomuurit pystyvät käsittelemään enemmän verkkoliikennettä samassa ajassa kuin toiset. (Andrés & Kenyon 2004, 434) Palomuuri ei suojaa yrityksen sisällä tapahtuvia toimintoja, kuten tietojen kopioimista ulkoiselle massamuistille.

## 6.2 Reititin

Palomuurissa voi olla reititin integroituna, mutta tällaiset palomuurit eivät ole kaikkein tietoturvallisimpia ratkaisuita (Kajala 2002, 205). Tämän vuoksi erillisen reitittimen olemassaolo on perusteltua. Reititin mainostaa yrityksen verkkoa muualle Internetiin. Reitittimen kautta on mahdollista päästä mihin tahansa yrityksen lähiverkon sisällä. (Malik 2003, 708) Kryptaamalla tulee suojata yhteydet reitittimeen, kun ylläpito ottaa siihen yhteyden. Tätä ennen pitää suorittaa käyttäjän varmentaminen. (Malik 2003, 58) Reitittimen käyttämättömät palvelut tulee poistaa kokonaan käytöstä (Malik 2003, 62).

### 6.2.1 IPSec

IPSec eli Internet protocol security architecture on ainoa Internetin suojaustekniikka, joka toimii kaikissa Internetin tiedonkulun protokollissa. IPSecin avulla varmistetaan kahden laitteen välinen turvallinen yhteydenpito. IPSec mahdollistaa tiedon salauksen, osapuolten todennuksen ja tiedon eheyden. (Doraswamy & Harkins 2003, 43-44) Kaikki turvallisuuteen liittyvät toimenpiteet tehdään yhdessä paikassa. Eri ohjelmia ei siis tarvitse erikseen suojata. IPSecin avulla voidaan suojata virtuaalinen etäyhteys tai lähiverkko. (Doraswamy & Harkins 2003, 167) Toiset Internetiin liittyvät protokollat voivat aiheuttaa ongelmia IPSecille. Todennäköisempää kuitenkin on, että IPSec aiheuttaa ongelmia niille. (Doraswamy & Harkins 2003, 217)

### 6.2.2 NAC

NAC eli network access control estää kaikki epäilyttävät tiedonsiirrot verkkoliikenteestä. Huomatessaan epäilyttävää liikennettä, NAC estää sen ja käyttäjä ohjataan sallittuun verkkoon. NAC etsii myös haittaohjelmia ja niiden asetuksia käyttäjän laitteelta, kun käyttäjä kirjautuu sisään NACiin. Huomatessaan jotain poikkeavaa normaalista, NAC poistaa käyttäjän verkosta. (Clark 2008, 20) Käyttäjät voivat tuoda verkkoon oman laitteensa. Laite pitää kuitenkin rekisteröidä NAClle ennen kuin se toimii verkossa. Uutta rekisteröintiä ei tarvita saman laitteen kohdalla. (Clark 2008, 15) NAC ei salli verkossa muita kuin siihen rekisteröityjä laitteita (Clark 2008, 22). NAC lisää yhden uuden suojaustason yrityksen lähiverkkoon palomuurin ja muiden suojauksien kanssa. NAC ei ole välttämättömyys kaikissa verkoissa. Ennen kuin NAC otetaan käyttöön jossain verkossa, pitää tietää NACiin liittyvät vaatimukset, koska se ei välttämättä ole paras ratkaisu kaikkeen. NACin toimintaperiaatteet pitää olla valmiiksi mietittyinä, kun NAC otetaan käyttöön. Tällä tavalla NACin asetuksien säätäminen on helpompaa. Kolmas tärkeä asia on muistaa, mitä kannattaa suojata NACin avulla. (Clark 2008, 39)

# 7 ETÄTYÖT

## 7.1 VPN

VPN on virtuaalinen etäkäyttöyhteys, jonka avulla yhdistetään vähintään kaksi työasemaa samaan verkkoon. VPN mahdollistaa turvallisen tietokoneen käytön kun esimerkiksi selataan Internetiä tai luetaan sähköpostia tietokoneen ollessa julkisessa verkossa (Laaksonen, Nevasalo & Tomula 2006, 168). Samalla periaatteella yrityksen toimihenkilö pääsee käsiksi kotoaan kotikoneellaan yrityksen palvelimiin tietoturvallisesti. VPNää voidaan hyödyntää yrityksessä myös extra- ja intranettinä. (Feilner 2006, 9) Sähköpostia luettaessa muualta kuin yrityksen sisältä, esimerkiksi kotoa, on suojaamiseksi käytettävä VPN–yhteyttä tai Web Mailia, joka on suojattu HTTPS–yhteydellä (Laaksonen, Nevasalo & Tomula 2006, 197-198).

VPN auttaa salauksellaan varmentamaan tiedon luottamuksellisuuden, eheyden ja saatavuuden. Luottamuksellisuudella tarkoitetaan tiedon saatavuutta vain niille, joille se kuuluu. Eheydellä tarkoitetaan sitä, että tieto ei muutu lähettäjän ja vastaanottajan välillä. Tiedon saatavuudella tarkoitetaan, että tieto on varmasti tallella, ja että siihen pääsee helposti käsiksi kun tietoa tarvitaan. (Feilner 2006, 17)

VPN tarvitsee toimiakseen kolme asiaa. Ensimmäinen vaatimus on, että palomuurista löytyy VPNää tukeva ominaisuus. Seuraava vaatimus on erillinen tai palomuurin oma VPN -ohjelma. Kolmas ja viimeinen vaatimus muodostaa verkosta salatun. Verkko tietokoneiden välillä salataan käyttämällä erityisiä salaukseen käytettäviä avaimia. Tieto siis muunnetaan salatuksi ennen siirtoa toiselle koneelle, jossa tiedon salaus puretaan. Vain avaimenhaltija voi salata ja avata salauksen. (Feilner 2006, 8-9)

## 7.2 WLAN

WLAN on langaton lähiverkko. WLANiin liitetyt laitteet eivät siis tarvitse verkkokaapeleita päästääkseen Internetiin. Samalla WLANin turvallisuus heikentyy, koska ei ole fyysistä estettä verkkoliikenteelle. WLANit ovat helppoja asentaa ja käyttää.

Tämän kaiken vuoksi ne ovat niin yleisiä. Yleisin WLAN standardi on 802.11. (Leary & Roshan 2004, 21)

802.11 standardissa havaittiin puutteita käyttäjien todentamisessa ja salauksessa kun se julkaistiin. WLANin todentamiskeinot ovat erittäin vajavaiset. WLAN on salattava siis jollakin muulla keinolla tai muuten verkko on todella vaarallinen käyttää, koska ketään käyttäjistä ei voida todentaa varmuudella. (Leary & Roshan 2004, 126) WLAN voidaan suojata kahdella eri salauksella. WEP eli wired equivalent privacy on salauksista heikoin, mutta antaa kuitenkin jonkin verran suojaa. WLAN pitää salata WPAn eli Wi-Fi Protected Accessin avulla, mikäli hakkeri on kokeneempi ja määrätietoisempi. WPAn salaus on toimivampi, koska se käyttää datan salaukseen väliaikaista avainta, toisin kuin WEP. (Cox 2003, 28)

WLANin käyttöä suunniteltaessa pitää siis huomioida, että verkko on tarpeeksi hyvin salattu. Yhtenäiseen laitteistoon ja tukiasemien sijoittamiseen ja niiden antenneihin pitää myös kiinnittää huomiota. Yhtenäinen laitteisto auttaa ylläpidossa. Tukiasemien antennien pitää kantaa tarpeeksi yrityksen sisätiloissa, koska seinät ja lattia voivat estää tiedonvälityksen kokonaan. Tällöin voidaan kuitenkin myös käyttää toista tukiasemaa. Yrityksen omassa käytössä voisi olla salattu WLAN omassa virtuaalisessa lähiverkossaan. Salaamaton WLAN voisi olla asiakkaiden ja huollon väliaikaisessa käytössä. Tämän WLANin voisi sijoittaa omaan erilliseen virtuaaliseen lähiverkkoon erilleen salatusta WLANista ja yrityksen muusta verkosta. WLANiin kirjautuessa voidaan käyttää NACia apuna (Clark 2008, 33).

## 7.3 PED-laitteet

PED muodostuu sanoista personal electronic device eli suomeksi tarkoitetaan henkilökohtaisia elektronisia laitteita. (Laaksonen, Nevasalo & Tomula 2006, 218) PED–laitteita ovat esimerkiksi kannettavat tietokoneet, PDA–laitteet, muistitikut, flash–muistit, MP3-soittimet ja kännykät. PED–laitteiden tietoturva on oltava yhtä hyvässä kunnossa kuin muidenkin laitteiden. (Laaksonen, Nevasalo & Tomula 2006, 162) Lisäksi laitteet tulee päivittää kun niihin on saatavilla päivityksiä, muuten ne ovat vieläkin haavoittuvaisempia. (Laaksonen, Nevasalo & Tomula 2006, 221)

PED–laitteiden käsittelyssä on huomioitava seuraavat asiat:

- mitä tietoa näillä laitteilla saa säilyttää
- miten tietoliikenneyhteydet suojataan
- mitä tehdä, jos laite tai media katoaa tai menee rikki
- miten tieto varmistetaan ja varmuuskopioidaan
- miten käyttöä valvotaan
- miten laitteita kuljetetaan ja säilytetään (tärinä ja lämpötilan vaihtelu) (Laaksonen, Nevasalo & Tomula 2006, 162, 168-169)

Biometrinen tunnistus eli sormenjälkitunnistus on hyödyllinen ja helppo tapa estää tuntemattomia pääsemästä laitteessa oleviin tietoihin käsiksi. (Laaksonen, Nevasalo & Tomula 2006, 220) Muistitikuissa pitäisi olla tiedon salauksen mahdollistama kryptausmenetelmä. Salausohjelmiston tärkeimmät vaatimukset ovat: helppokäyttöisyys, kaiken laitteella olevan tiedon salaus sekä keskitetyn ylläpidon tukeminen. Helppokäyttöisyydellä tarkoitetaan, että järjestelmään kirjautuminen on riittävä toimenpide, eikä muita salaukseen liittyviä toimenpiteitä tarvitse tehdä. Keskitetyllä ylläpidolla tarkoitetaan käyttäjä-salasanaparien uusimista tarpeen mukaan ja laitteen itsensä automaattista lukitsemista määräajan umpeutuessa. PED–laitteiden verkkoturvallisuuden kannalta merkittäviä toimenpiteitä ovat käyttämättä olevien Bluetooth- ja WLAN–yhteyksien käytöstä poistaminen kun niitä ei tarvita. (Laaksonen, Nevasalo & Tomula 2006, 221)

# 8 TÄRKEÄN TIEDON KÄSITTELY

”Organisaation toiminnan kannalta kaikki omaisuus ja sen merkitys on oltava tarkassa tiedossa, oli tämä omaisuus kiinteässä muodossa tai tieto-omaisuutta.” (Tammisalo 2005, 29)

Ennen kuin tietoa voidaan käsitellä oikein, on se luokiteltava ensin. Yrityksen työntekijöiden on tiedettävä, että he käsittelevät yrityksen toiminnan kannalta merkittävää ja arvokasta tietoa. Luokittelu helpottaa tiedon käsittelyä. Tietoja voidaan luokitella

seuraavalla periaatteella. Ensiksi tiedolle valitaan luokka mihin se kuuluu. Tieto voi olla luottamuksellista tai julkista. Seuraava vaihe on tiedon käsittelyn periaatteet. Miten tietoa käsitellään kirje-, sähköpostina ja puhelimen välityksellä? Seuraava tarvittava toimenpide liittyy tiedon salaukseen. Onko käsiteltävä tieto salattava? Viimeinen tiedon käsittelyn vaihe on sen hävittäminen. Luottamuksellista tietoa ei pidä heittää normaaliin roskikseen, vaan pistää silppurista läpi tai mieluummin käyttää erillistä tietoturvaroskalaatikkoa. (Laaksonen, Nevasalo & Tomula 2006, 161) Yrityksen kaikkien henkilöiden tulee noudattaa näitä sääntöjä käsitellessään tietoja.

## 8.1 Elektroninen tieto

Elektroninen tieto ei ole välttämättä näkyvillä fyysisessä muodossa, kuten esimerkiksi tulostettu kopio sähköpostiviestistä. Yrityksen järjestelmien hallintaan, tiedonsiirtoon ja ylläpitoon liittyvät yhteydet, selainpohjaiset järjestelmät, missä käyttäjältä vaaditaan tunnistautuminen tai tehdään ostotapahtuma, sähköpostiviestien lähettäminen, tiedon varastoiminen ja etäkäyttöyhteydet on salattava, muuten kolmas osapuoli voi päästä tietoihin käsiksi. (Laaksonen, Nevasalo & Tomula 2006, 195-196) Jos tietokoneen kiintolevy ei ole salattu, ja ulkopuolinen henkilö saa sen haltuunsa, on mahdollista lukea koko kiintolevy. Käyttäjätunnukset ja salasanat voidaan selvittää nopeasti, mutta jos kiintolevy on salattu, sen sisältämää tietoa ei voida lukea. Nykypäivän salausmenetelmillä tietokoneen käyttö ei hidastu ollenkaan salauksen ollessa päällä. Kiintolevyn salausmenetelmänä käytetään erillistä salaukseen tarkoitettua salausohjelmistoa. (Laaksonen, Nevasalo & Tomula 2006, 196) Järjestelmien ylläpitoyhteyksiin on käytettävä salattua protokollaa. Jos järjestelmiä on ulkoistettu, on myös niiden järjestelmien yhteydet oltava salattuja. Salaavia protokollia ovat: SSH, HTTPS, SFTP ja SNMP. (Laaksonen, Nevasalo & Tomula 2006, 196)

Elektronisen tiedon säilytyksessä pitää olla huolellinen, etteivät siihen pääse käsiksi muut kuin yrityksen työntekijät. Elektronisen tiedon säilytys on haastavampaa kuin fyysisen tiedon, koska fyysiseen tietoon on ulkopuolisen vaikeampi päästä käsiksi. Erilaisia säilytystapoja elektroniselle tiedolle ovat omat ja kolmannen osapuolen palvelimet, CD- ja DVD–levyt ja ulkoiset kiintolevyt. Elektronisen tiedon säilytyspaikka tulee olla uudenaikainen. Vanhoilta tallenteilta tieto tulee siirtää uudenaikaisille

tallenteille. Varastossa olevan elektronisen tiedon voi pakata pienemmäksi, ettei se vie turhaa tilaa säilytyskohteessaan. Useammin tarvittavan elektronisen tiedon pakkausta ei kannata harkita, koska pakkaustapahtumat vievät tällöin turhaa aikaa. Elektronisen tiedon säilytysaika vaihtelee sen tärkeyden ja vaihtuvuuden mukaan. Data tulee salata ennen tallentamista tai vastaavasti tallenne, jonne data tulee, tulisi salata.

Kiintolevyn alustaminen ei poista tietoja kiintolevyltä kokonaan, vaan tieto todennäköisesti jää levylle talteen. On mahdollista, että tiedon saa palautettua erilaisilla tiedonpalautusohjelmilla. Jos tieto halutaan tuhota pysyvästi kiintolevyltä, pitää ylikirjoittaa kiintolevy moneen kertaan uudelleen. Tähänkin tarkoitukseen on olemassa erilaisia ohjelmia. (Baum & McDaniel 2009, 26-27) Muita kiintolevyn tuhoamistapoja ovat voimakas magneetti kiintolevyn kylkeen tai kiintolevyn totaalinen fyysinen tuhoaminen.

## 8.2 Fyysinen tieto

Fyysistä tietoa on esimerkiksi kirjepostina tullut lasku. Fyysistä tietoa tulee säilyttää paloturvallisessa paikassa. Ulkopuolisen henkilön pääsy fyysisen tiedon arkistointipaikkaan tulee estää kulunvalvonnalla. Fyysisen tiedon arkistoinnissa kannattaa pitää jonkinlainen järjestys, kuten aika- tai aakkosjärjestys, jotta arkistoitu dokumentti löytyy helpommin.

Rypistämätön paperi vie vähemmän tilaa roska-astiassa kuin rypistetty. Roskakoria ei tarvitse tyhjentää yhtä usein tällä tavalla. Tieto ei häviä paperia rypistämällä. (Laaksonen, Nevasalo & Tomula 2006, 162) Tietoturvaroskalaatikot tai papereiden hallittu polttaminen ovat hyviä tapoja päästä eroon tärkeistä fyysisistä tiedoista.

## 8.3 Asiakkaiden tiedostojen kopiointi ja säilytys

Asiakkaan tietokoneelta on otettava tärkeät tiedot talteen kun esimerkiksi tietokoneen kiintolevy on rikkoutunut tai käyttöjärjestelmä on mennyt sekaisin. Tärkeitä tietoja ovat esimerkiksi valokuvat ja dokumentit. Hyvä tiedostojen kopiointitapa on siirtää

asiakkaan tiedot ulkoiselle kiintolevylle huoltotöiden ajaksi. Tällä tavalla asiakkaan tärkeät tiedot eivät ole vaarassa hävitä.

Ulkoinen kiintolevy, jolle tiedot tulevat, on oltava kapasiteetiltaan riittävän tilava, jotta tiedot mahtuvat sinne. Kyseinen kiintolevy olisi oltava salasanalla suojattu ja kiintolevyn sisältö kryptattu. Tämän kiintolevyn fyysinen sijoituspaikka ei saa olla ulkopuolisten henkilöiden saatavilla, ei edes asiakkaan, jonka tietoja kiintolevy sisältää, koska siellä on muidenkin asiakkaiden tietoja. Asiakkaiden tiedostoja ei tulisi säilyttää turhaan. Tiedostot tulee poistaa kiintolevyltä, kun asiakas on noutanut tietokoneensa huollosta ja on todennut, että tiedostot ovat palautettuna tietokoneellaan.

# 9 SALASANAT

## 9.1 Salasanojen merkitys

Omaa salasanaa eikä käyttäjätunnusta saa koskaan kertoa toiselle henkilölle. Jokaisella käyttäjällä pitää olla oma salasana. Liian monta eri salasanaa on vaikea muistaa, ja koska salasanoja ei pidä kirjoittaa muistiin minnekään, ovat yrityksen järjestelmät suunniteltava siten, että ei olisi tarvetta kuin yhdelle käyttäjätunnus-salasanaparille. Lisäksi yrityksen on suunniteltava ja päätettävä, mitkä ovat toimenpiteet, jos salasana unohtuu, katoaa, päätyy vääriin käsiin tai se on syötetty liian monta kertaa. (Laaksonen, Nevasalo & Tomula 2006, 166-167) Työpaikan salasanaa ei tulisi käyttää yrityksen ulkopuolella yksityiskäytössä (Pulliainen 2011, 25).

## 9.2 Vahvat salasanat

Vahvat salasanat sisältävät pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä. Salasana ei saa olla liian lyhyt, mitä pidempi salasana sitä vahvempi se on. Hyvän salasanan pituus on kahdeksan merkkiä. Salasana ei saa olla sama joka paikassa, ja se tulee uudistaa usein. (Laaksonen, Nevasalo & Tomula 2006, 166) Oma nimi, lemmikin nimi, salasana, password, 0000, 1234 ovat esimerkkejä huonoista salasanoista.

### 9.3 Salasanojen uudistaminen

Käyttäjän pitää muuttaa oletussalasana aina ensimmäiseksi kun hän kirjautuu uuteen järjestelmään tai sovellukseen. (Laaksonen, Nevasalo & Tomula 2006, 167) Salasanoja voidaan uudistaa esimerkiksi seuraavalla tavalla:

1. Valitaan kaksi sanaa: ”pakastin toimii”
2. Lisätään alaviiva sanojen väliin: ”pakastin_toimii”
3. Vaihdetaan muutama pieni kirjain isoiksi: ”PakasTin_ToiMii”
4. Muutetaan kirjaimia numeroiksi: ”PakasT1n_To1M11”
5. Lisätään vielä yksi erikoismerkki: ”Paka$T1n_To1M11”
6. Salasana on valmis

Samaa kahden sanan yhdistelmää voidaan uudistaa pienillä muutoksilla tarpeen vaatiessa esimerkiksi lisäämällä numeroita sanojen perään tai vaihtamalla isojen kirjaimien paikkaa.

## 10 LAITTEIDEN HUOLTO

Yrityksen laitteita on huollettava säännöllisesti. Huoltotoimenpiteissä on noudatettava laitevalmistajan suosituksia. Helpoin ja yksinkertaisin huoltotoimenpide on laitteiden puhdistaminen säännöllisesti. Laitteita ei tulisi huoltaa kenenkään muun kuin siihen työhön koulutettujen henkilöiden. Mikäli yrityksen laite on lähetettävä huollettavaksi yrityksen ulkopuolelle, on huomioitava kuljetuksenaikainen suojaus. Huomioitavaa tällöin ovat erilaiset fyysiset vahingot, tärinä, varkaudet ja tapaturmat. Tämän takia pääsy mahdollisiin tietoihin on estettävä tai siirtämällä tieto toiselle muistivälineelle kunnes tiedot voidaan palauttaa korjatulle laitteelle. (Tammisalo 2005, 48-49) Tällöin ei tarvitse huolehtia yritys- tai muiden salaisuuksien leviämistä huollon aikana. Samalla tavalla hoidetaan asiakkaiden huoltoa tarvitsevat laitteet, joita ei voida korjata yrityksen tiloissa.

## 10.1 Laiterikot

Laitteet voivat mennä rikki erilaisista syistä. Jos jokin laite menee, on hyvä olla suunnitelma kaiken varalta. Mokkula on esimerkiksi hyvä varayhteys, kun Internetiin liittyvä laitteisto on poissa käytöstä syystä tai toisesta. Palomuurit, reitittimet ja muut verkkolaitteisto olisi hyvä olla peilattuina identtisille laitteille. Jos laite menee rikki, peilattu varalaite tulee rikkoutuneen laitteen tilalle automaattisesti. Mikäli tämä ei ole mahdollista, niin varalaite tai jokin toinen väliaikainen ratkaisu pitää olla selvillä. Kiintolevyn rikkoutuessa tietokone tulee sulkea välittömästi ja irrottaa kiintolevy. Tämän jälkeen kiintolevyn voi liittää toiseen tietokoneeseen ja kokeilla onko mahdollista saada tärkeät tiedot kopioitua varmempaan talteen. Mikäli tämä ei onnistu, pitää miettiä, onko kiintolevyn sisällä oleva tieto niin tärkeää, että se pitää viedä kolmannelle osapuolelle tiedonpalautukseen.

## 10.2 UPS

UPS on virransyöttöjärjestelmä. Sen tärkeimpiä tehtäviä ovat antaa siihen liitetyille laitteille varavirtaa hetkellisesti sähkökatkon sattuessa ja turvata laitteet sähköverkon virtapiikeiltä, esimerkiksi ukkoselta. UPS -laite sijoitetaan laitteen ja virtalähteen välille. Jokainen palvelin, jonka tärkeysluokaksi on määritelty ”kriittinen” tai ”tärkeä”, pitää olla kiinni UPS -laitteessa. Sähkökatkon sattuessa UPSn pitää tuottaa varavirtaa tarpeeksi, jotta siihen liitetyt palvelimet ehtisivät suorittamaan omat tarpeelliset toimenpiteet ennen sulkeutumista. Hyvä varavirran kestoaika on noin viisitoista minuuttia. UPS -laitteiden toimintakyky on säännöllisesti testattava.

# 11 TIETOTURVARISKIN TOTEUTUESSA

Kun yrityksen työntekijä huomaa tietoturvariskin toteutuneen, hänen on otettava välittömästi yhteyttä yrityksen tietoturvasta vastaavaan henkilöön. Tietoturvasta vastaava henkilö raportoi riskin aiheuttamasta haitasta asiaankuuluvalle viranomaiselle tai taholle. Jokainen Mikropasin työntekijä on vastuussa, siitä että hän noudattaa kaikkia tietoturvaohjeita. Toimintaohjeita erilaisten tietoturvariskien toteutumiselle löytyy liitteestä 1. Tietoturvariskin toteutuessa tärkeimmät asiat ovat palvelun jatkuvuus ja toipuminen. Mikäli tietoturvariskejä toteutuu useita yhtä aikaa, tärkeimmät osa-alueet saavat tällöin suuremman prioriteetin. Suuremman prioriteetin saaneiden riskien haittavaikutukset on voitettava mahdollisimman nopeasti, jotta muutkin toteutuneet riskit saadaan hoidettua. Tärkeysjärjestyksessä ensimmäisenä on data eli laitteiden sisältämä tieto. Tiedon jälkeen tärkeysjärjestyksessä tulevat vasta itse laitteet.

# 12 TOIPUMINEN

Yrityksen tulisi laatia toipumissuunnitelma, ellei sillä sitä jo ole. Toipumissuunnitelman tulee sisältää seuraavat asiat:

- Riskin realisoituessa tehtävät toimenpiteet
- Tutkia ja selvittää haavoittuneet järjestelmät
- Välittömien ja välillisten haittojen selvittäminen riskin toteutuessa
- Toimenpiteet vahinkojen pienentämiseksi
- Vastuuhenkilön nimeäminen
- Toipumiseen tarvittava aika

”Toipumissuunnitelmaa tarvitaan silloin, kun liiketoiminnan kannalta on tapahtunut jotain sellaista, joka vakavasti häiritsee tai jopa estää normaalin liiketoiminnan.” Toipumissuunnitelma pitää olla harjoiteltu ja testattu ennen kuin jotain tapahtuu. (Laaksonen, Nevasalo & Tomula 2006, 234) Yksi tärkeä määriteltävä asia toipumissuunnitelmaa laadittaessa on, se koska suunnitelma tulee aktiiviseksi (Laaksonen, Nevasalo & Tomula 2006, 236).

## 12.1 Varmuuskopiointi

Yrityksen tiedot on varmuuskopioitava yllättävien tilanteiden varalta. Tiedon tulee säilyä luotettavana ja siihen on päästävä helposti käsiksi. Mitä tärkeämpi tieto on, sitä nopeammin se on varmuuskopioitava, kun siihen on mahdollisuus. Varmuuskopioinnin on parempi olla automaattista, koska käyttäjät eivät sitä kuitenkaan aina muista tehdä. (Laaksonen, Nevasalo & Tomula 2006, 170-171) Automaattinen varmuuskopiointi on oltava mahdollisimman huomaamaton. Salaamattomat ja salatut tiedot on varmuuskopioitava (Laaksonen, Nevasalo & Tomula 2006, 161). Varmuuskopiointia tulee kaivanneeksi jos sitä ei ole, kun esimerkiksi kiintolevyltä kaikki tieto on kadonnut. Paras ajankohta varmuuskopioinnille on yöaika, koska silloin varmuuskopiointilaitteet aiheuttavat vähiten haittaa käyttäjille. Tallennetun tiedon hallinnointi on vaikeaa, jos tietoa tallennettaan moniin kohteisiin. Tämän takia keskitetty ratkaisu on tärkeää. Kun tieto on saatu varmuuskopioitua, tulee testata saadaanko varmuuskopioitu tieto palautettua ja voidaanko sitä käyttää (Laaksonen, Nevasalo & Tomula 2006, 170). Varmuuskopioinnin säilytyspaikka voi olla yrityksen oma sisäinen ratkaisu tai Internetin kautta sijaitsevalla erillisellä palvelimella, jota myös kutsutaan pilveksi.

### 12.1.1 NAS

NAS on liitettynä lähiverkkoon ja se hyödyntää tiedonsiirrossaan samoja verkkokaapeleita kuin muukin lähiverkko. Lähiverkon muut Internetiin liitetyt koneet voivat joutua rasituksen alle, koska NAS käyttää Internetiin liittyviä protokollia, kuten TCP/IPtä. NASn asennus ja ylläpito ovat helposti tehtävissä, joten aikaa näihin toimenpiteisiin ei tarvita niin paljon kuin SANin. NASn avulla pilvessä sijaitsevaan varmuuskopiointipalvelimeen voi olla yhteydessä useita eri koneita samaan aikaan. NAS on hitaampi tekemän varmuuskopion kuin SAN. (Gupta 2002, 29) NAS on yritykselle kalliimpi ratkaisu kuin SAN, mutta riskit varmuuskopioinnissa ovat kolmannella osapuolella. Pienille määrille tallennettavaa ja käytettävää tietoa paras ratkaisu on siis NAS (Ogletree 2004, 181).

### 12.1.2 SAN

Mikäli yrityksellä on oma sisäinen ratkaisu, sen pitää muistaa, että varmuuskopioidun tiedon säilytyspaikka on oltava paloturvallinen (Laaksonen, Nevasalo & Tomula 2006, 170). SAN toimii lähiverkossa kuten NAS, mutta SAN ei kuormita verkkoliikennettä, koska se on omana verkkonaan (Ogletree 2004, 180). SAN tarvitsee jonkin verran osaamista asennuksessaan ja ylläpidossaan, joka tekee SANsta kalliin ratkaisun (Gupta 2002, 29). SAN on hyvä ratkaisu, mikäli tallennettavaa tietoa on paljon ja tietoon tarvitsee päästä käsiksi useasti. (Ogletree 2004, 181) Muita sisäisiä ratkaisuita voivat olla esimerkiksi ulkoiset massamuistit, mutta niiden käytölle pitää olla erittäin hyvät perusteet, koska ne eivät ole lähellekään yhtä luotettavia ja tietoturvallisia kuin edellä mainitut ratkaisut. Kaikissa yrityksen ulkoisissa massamuisteissa on oltava tiedon salausmenetelmät kunnossa jos niissä on yrityksen tietoja.

# 13 TIETOTURVASUUNNITELMAN KÄYTTÖÖNOTTO

Ennen kuin tietoturvasuunnitelma voidaan ottaa käyttöön, se pitää testata toimivaksi. Paras mahdollinen testauspaikka on jokin yksityinen testauksiin erikoistunut yritys. Tämä ei välttämättä ole kuitenkaan mahdollista, joten yrityksen pitänee testata tietoturvasuunnitelmaa itsenäisesti. Testaaminen ei voi kuitenkaan tapahtua yrityksen aukioloaikoina, koska testaamisen aikana tapahtuvat muutokset voivat sekoittaa nykyisiä järjestelmiä, ja tällä tavalla aiheuttaa hankaluuksia. Testaukselle paras aika on silloin, kun liiketila ei ole avoin asiakkaille.

Tämä tietoturvasuunnitelma otetaan käyttöön vaiheittain, yrityksen haluamalla tavalla. Jotkin osa-alueet ovat jo olleet aikaisemmin kunnossa. Yrityksellä on tämän työn jälkeen paremmat valmiudet päivittää loputkin tietoturvaan liittyvät asiat viimeisen päälle kuntoon. Käyttöönoton yhteydessä on hyvä dokumentoida siirtyminen vanhasta uuteen. Dokumentointi helpottaa muistamista, kun seuraavan kerran tarvitaan vastaavaa uudistamista. Dokumentoinnissa on huomioitava hyvin ja huonosti menneet kohdat ja asiat, jotka voidaan tulevaisuudessa parantaa.

Tietoturvasuunnitelmaa käyttöönotettaessa on huomioitava mahdolliset muutokset henkilökunnan tottumiin tapoihin hoitaa asioita. Näihin muutoksiin on annettava riittävä määrä koulutusta ennen ja jälkeen tietoturvasuunnitelman käyttöönoton. Henkilökunnan koulutuksessa voi hyödyntää tätä dokumenttia.

# 14 TIETOTURVASUUNNITELMAN SEURANTA JA PÄIVITYS

Tietoturvasuunnitelman testaaminen on osa sen seurantaa. Tietoturvasuunnitelman osa-alueet tulisi testata säännöllisesti mahdollisimman laajalti ja tuloksista tulisi tehdä raportti. Mahdolliset puutteet tulisi korjata niiden tärkeyden vaatimalla aikataululla. (Laaksonen, Nevasalo & Tomula 2006, 150) Yrityksen on määriteltävä kuka vastaa tietoturvasuunnitelman toteuttamisesta ja keitä se koskettaa (Laaksonen, Nevasalo & Tomula 2006, 128). Tietoturvasuunnitelman toteuttamisesta vastaavalta henkilöltä edellytetään tehokasta valvontaa ja ohjausta tietoturvallisuuden edistämiseksi ja kehittämiseksi yrityksen sisällä.

Tämän tietoturvasuunnitelman tekeminen oli kertakäyttöinen projekti. Tulevaisuudessa tietoturvasuunnitelman päivittämisestä tulee yrityksen itse vastata. Tietoturvasuunnitelman kehittäminen on jatkuva prosessi, jota täytyy päivittää ja kehittää säännöllisin väliajoin. (Tammisalo 2005, 9)

# 15 YHTEENVETO

Tietoturvasta tullee monelle mieleen ensimmäisenä virukset, mutta näin yksinkertainen tämä tietoturvaan liittyvä alue ei tietenkään ollut. Tietoturvasuunnitelmasta tuli kattava kokonaisuus, jossa on huomioitu, miten voidaan ennaltaehkäistä nykypäivän tietoturvauhkia. Tämä opinnäytetyötyö Mikropasille soveltuu myös muille saman suuruusluokan kokoisille yrityksille.

Tätä työtä tehdessäni olen vahvistanut entuudestaan tuttuja tietojani ja osannut hahmottaa uusia kokonaisuuksia. Uusia ideoita ja mahdollisuuksia tuli esiin koko ajan, kun suunnittelin ja tein kirjallista osiota. Aiheeseen liittyvää kirjallisuutta on saatavilla ihan mukavasti, mutta niiden sisältö ei aina ollut nykypäivän standardien mukaista. Alalle tulee koko ajan uutta tekniikkaa, joka vaikeuttaa perässä pysymistä. Suomenkielistä kirjallisuutta ei ole saatavilla paljoa, mutta se on sitten sitäkin laadukkaampaa. Internetistä saa kaiken tarvittavan tiedon, mutta se on hajallaan, eikä sen laadusta voi aina olla varma.

Tämä tietoturvasuunnitelma on vain teoriaa, kuten kaikki muukin kirjoitettu teksti, pitää myös toimia sen mukaisesti. Heikkoutena on, että tietoturvasuunnitelma ei takaa mitään, ellei sitä noudateta. Suunnitelman vanhenemista voidaan pitää uhkana, ellei sitä päivitetä säännöllisin väliajoin. Tietoturvasuunnitelma ei ainoastaan mahdollista vankkaa tukijalkaa tietoturvauhkia vastaan, vaan parantaa myös yrityksen imagoa turvallisena ja ajanmukaisena yrityksenä.

# LÄHTEET

Andrés, S. & Kenyon, B. 2004. Security Sage's guide to hardening the network infrastructure. Rockland Syngress Publishing, Inc.

Angelescu, S. 2010. CCNA Certification All-In-One for Dummies. Indianapolis Wiley Publishing, Inc.

Baum, N. & McDaniel, J. 2009. Disaster Planning for the Clinical Practice. USA Jones and Bartlett Publishers, LLC

Beekelaar, R., Komar, B. & Wettern, J. 2003. Firewall for Dummies, 2nd Edition. Indianapolis Wiley Publishing, Inc.

Blokdijk, G. & Menken, I. 2008. Virtualization - The Complete Cornerstone Guide to Virtualization Best Practices. Emereo Pty Limited

Cantrell, C., Lucas, M. & Abhishek, S. 2006. Firewall policies and VPN configurations. Rockland Syngress Publishing, Inc.

Carswell, R. & Webb, H. 2009. Guide to Microsoft Virtual PC 2007 and Virtual Server 2005. Boston Cengage Learning, Inc.

Clark, D. 2008. Network Access Control 100 Success Secrets. Emereo PTY LTD

Cox, J. 2003. WLAN security: A big problem for small nets. Network World 1.9.2003

Doraswamy, N. & Harkins, D. 2003. IPSec The New Security Standard for the Internet, Intranets, and Virtual Private Networks. New Jersey Prentice Hall PTR

Feilner, M. 2006. OpenVPN: Building and Integrating Virtual Private Networks. 1. p. Birmingham Packt Publishing

Feit, S. 2000. Local area high speed networks. Indianapolis MTP

Gupta, M. 2002. Storage area network fundamentals. Indianapolis Cisco Systems, Inc.

Jakobsson, M & Myers, S. 2007. Phising and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. New Jersey John Wiley & Sons, Inc.

Kajala, T. 2002. Hakkerin käsikirja. Helsinki Edita Prima Oy

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. 1. p. Helsinki EDITA

Leary, J. & Roshan, P. 2004. 802.11 Wireless LAN fundamentals. Indianapolis Cisco Press

Leiden, C., Wilensky, M. & Bradner, S. 2009. TCP/IP for Dummies, 6th Edition. Indianapolis Wiley Publishing, Inc.

Malik, S. 2003. Network security principles and practices. Indianapolis Cisco Systems, Inc.

Ogletree, T.W. 2004. Upgrading and repairing networks. USA Que Publisinhg.

Pulliainen, M. 2011. Tietoturvan pyhä kolminaisuus. Satakunnan Kansa 6.2.2011.

Pulliainen, M & Suojanen, S. 2011. Tietoturva unohtuu uusien vimpainten kanssa. Satakunnan Kansa 6.2.2011.

Shelly, G. & Vermaat, M. 2009. Discovering Computers 2010: Living in a Digital World, Introductory. USA Cengage Learning, Inc

Singh S. 2009. Database Systems: Concepts, Design and Applications. Delhi Dorling Kindersley

Tammisalo, T. 2005. Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt. Stakes. Viitattu 27.1.2011. http://www.stakes.fi/verkkojulkaisut/raportit/Ra5-2005.pdf

Toivonen, A. 2002. Verkkotietoturvan hallinta - CERT. Helsinki Edita Prima Oy

Taulukko 2. Tietoturvaohjeet riskien toteutuessa

| Tietoturvariski | Selostus | Ohje | Prioriteetti |
|---|---|---|---|
| Haittaohjelmat | Virukset, madot ja kaikenlaiset muut haittaohjelmat | Saastunutta tietokonetta ei pidä sulkea. Haittaohjelma poistetaan haittaohjelman poistotyökalulla. | Keskisuuri |
| Ulkoiset uhat | Tiedon tai tuotteiden varastaminen, tunkeutuminen yrityksen lähiverkkoon tai tiloihin | Yhteys poliisiin | Korkea |
| Sisäiset uhat | Tahattomat tai tahalliset työntekijän tekemät luottamuksellisen aineiston paljastukset | Yhteys poliisiin | Matala |
| Tapaturmat ja onnettomuudet | Tulipalot, vesivahingot | Yhteys pelastuslaitokseen | Korkea |
| Häiriöt sähköverkossa | Sähkökatkot, virtapiikit ja ukkonen | Nopea, tärkeiden tietojen varmuuskopiointi sähkökatkon aikana UPS:n tuottaman varavirran avulla. | Korkea |
| Ihmisestä riippumattomat laitteistoon liittyvät uhat | Laiterikot ja tietokoneiden kaatumiset | Varalaite käyttöön tai rikkinäinen komponentti vaihdetaan tarvittaessa. Tietokone käynnistetään uudestaan sen kaatumisen jälkeen. | Keskisuuri |

| | | | |
|---|---|---|---|
| Ihmisestä riippuvat laitteistoon liittyvät uhat | Inhimilliset virheet laitteistoa käytettäessä, asentaessa tai korjattaessa | Suurempien haittojen estämiseksi on otettava yhteys laitteen huoltoon tai yhteyshenkilöön. | Matala |
| Datan eli tiedon häviäminen | Tahattomat tai tahalliset tiedostojen poistot | Poistettu tieto palautetaan varmuuskopion avulla | Matala |
| Tietoyhteyksien pettäminen | Internet- ja puhelinyhteyksien katkeaminen | Varayhteyksien aktivointi. | Keskisuuri |