TIETOTURVASUUNNITELMA PIENYRITYKSELLE

Kimmo Miettinen

Opinnäytetyö

Ammattikorkeakoulututkinto

Savonia
ammattikorkeakoulu

SAVONIA-AMMATTIKORKEAKOULU **OPINNÄYTETYÖ**
Tiivistelmä

Koulutusala Luonnontieteiden ala	
Koulutusohjelma Tietojenkäsittelyn koulutusohjelma	
Työn tekijä(t) Kimmo Miettinen	
Työn nimi Tietoturvasuunnitelma pienyritykselle	
Päiväys 13.10.2011	Sivumäärä/Liitteet 43
Ohjaaja(t) Granroth, Pekka	
Toimeksiantaja/Yhteistyökumppani(t) Salainen	

Tiivistelmä

Tämän opinnäytetyön aiheena oli laatia sähkö- ja tietojärjestelmäsuunnitteluun erikoistuneelle yritykselle tietoturvasuunnitelma. Suunnitelma tehtiin toimeksiantona rakennusalan yritykselle, mutta asioita on käsitelty yleisestä näkökulmasta. Tämän työn avulla muutkin yritykset voivat parantaa tietoturvansa tasoa ja laatia oman tietoturvasuunnitelman.

Opinnäytetyön aluksi kartoitettiin yrityksen nykyinen tietoturvan taso yrityksen tietoturvasta vastaavan henkilön kanssa. Kartoittaminen tehtiin tutkimalla yrityksen toimitilat, laitteisto ja toimintatavat. Löytyneet ongelmat ja puutteet kirjattiin ylös. Tämän jälkeen suunnitelman teko oli suoraviivaista.

Opinnäytetyö muodostuu kahdesta eri osasta. Ensimmäisenä on teoriaosuus, jossa käsitellään tietoturvan osa-alueet ja niihin liittyvät termit ja käsitteet. Työn toinen osa on yritykselle laadittu tietoturvasuunnitelma. Parannusehdotuksissa otettiin huomioon yrityksen todellinen tarve ja mahdolliset tulevaisuudessa tapahtuvat laajennukset.

Avainsanat
Tietoturva (YSA), palomuuri, tietoturvan osa-alueet

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Abstract

Field of Study Natural Sciences			
Degree Programme Degree Programme in Computer Science			
Author(s) Kimmo Miettinen			
Title of Thesis Information security plan for a small business			
Date	13.10.2011	Pages/Appendices	43
Supervisor(s) Granroth, Pekka			
Project/Partners Classified			

Abstract

The goal of this thesis was to create an information security plan for a company specialising in electrical- and information system design. The thesis was made as an assignment for building branch company, but the subject was approached from a general viewpoint. This thesis is usable for other companies, which want to improve their information security level or create an information security plan.

The starting point of this thesis was to map out the company's information security level together with the person in charge of information security. The company's business premises, hardware and policies were examined. Discovered problems and weaknesses were documented. After that, creating the plan was rather straightforward.

This thesis consists of two different parts. The first part is a theory section, where information on security is provided and common terms and concepts are explained. The second section contains an information security plan with suggestions for improvement. The company's real needs and possible future expansions were taken into account in the suggestions.

Keywords
Information security, firewall, information security sections

SISÄLTÖ

1 JOHDANTO

Nykyajan maailmassa tietotekniikkaa käytetään melkein kaikkialla ja se avaa yrityksille ainutlaatuisia mahdollisuuksia. Nämä mahdollisuudet tuovat mukanaan monenlaisia riskejä yrityksen liiketoiminnan kannalta tärkeille tiedoille. Yritysten on sisäistettävä, että yrityksen tietojen suojaus ei perustu pelkästään teknisiin välineisiin ja ohjelmiin, vaan terveellä järjellä, selkeästi laadituilla ohjeilla ja riittävällä työntekijöiden koulutuksella saadaan aikaan parhaat tulokset. (Symantec, 2007, 7.)

Tietoturvasta huolehtiminen on nykyaikana kaiken kokoisille yrityksille erittäin tärkeää, kuten yllä olevassa kappaleessa kerrotaan. Suuremmat yritykset ovat alkaneet panostaa tietoturvaan kunnolla, mutta pienemmissä yrityksissä asiat voivat olla heikolla mallilla. Suuria yrityksiä vastaan on tehty useita suunnattuja hyökkäyksiä, mikä on pakottanut yritykset parantamaan tietoturvaansa. Pienemmillä yrityksillä tietoturvaan panostaminen on ollut varsin pientä. Osa yrityksistä on keskittynyt ainoastaan tietoteknisiin asioihin, mutta tietoturvaan sisältyy paljon muitakin asioita. Yrityksen tietoturvan tason kartoittamisessa avuksi tulee tietoturvasuunnitelma, jonka avulla saadaan selville tietoturvassa ilmenevät puutteet.

Opinnäytetyön aiheena oli suunnitella ja toteuttaa tietoturvasuunnitelma sähkö- ja tietojärjestelmäsuunnittelua tarjoavalle yritykselle. Toimeksiantaja halusi, että opinnäytetyö tehdään salaisena, joten sen takia yrityksen nimeä tai tietoja ei työssä mainita. Suunnitelman tärkeimmät asiat oli selvittää yrityksen tämänhetkinen tietoturvan taso ja laatia mahdolliset korjausehdotukset. Toimeksianto tietoturvasuunnitelman tekoon tuli rakennusalan yritykseltä, mutta tietoturva-asioita käsitellään myös yleisestä näkökulmasta. Näin mikä tahansa pk-yritys voi käyttää suunnitelmaa apuna omassa tietoturvasuunnitelmassaan. Tietoturvan perusasiat ovat kuitenkin kaikille aloille samanlaiset. Opinnäytetyö rakentuu siten, että alussa käydään läpi tietoturvallisuuteen liittyviä käytänteitä, käsitteitä sekä laitteistoa ja työn lopussa on yritykselle laadittu tietoturvasuunnitelma.

.

2 TIETOTURVA

Tietoturvallisuuden määritelmä lähtee tietynlaisesta perusajatuksesta. Yrityksen tärkein omaisuus on tieto, joka on luotettavaa, oikeassa muodossa ja nopeasti saatavissa vain oikeille henkilöille. Tietoturvan perusmääritelmä rakentuu kuudesta eri osatekijästä:

- luottamuksellisuus
- käytettävyys
- eheys
- todennus
- kiistämättömyys
- pääsynvalvonta

Luottamuksellisuus (confidentiality) tarkoittaa sitä, että tietojärjestelmän sisältämät tiedot ovat vain niihin oikeutettujen henkilöiden käytettävissä. Käytettävyydellä (availability) tarkoitetaan sitä, että tiedot ovat aina saatavissa tietojärjestelmästä oikeassa muodossa ja riittävän nopeasti. (Rosendahl, 2011) Yksi tietoturvan vaikeimpia tehtäviä on käytettävyyden toteuttaminen. Eheydellä (integrity) tarkoitetaan laajasti ymmärrettynä sitä, että tietojärjestelmän sisältämät tiedot pitävät paikkansa eivätkä sisällä tahallisia tai tahattomia virheitä. Eheydellä voidaan myös tarkoittaa sitä, että tietoihin ei ole muutettu, poistettu tai lisätty mitään. (Hakala, Vainio & Vuorinen, 2006, 4)

Todennuksella (authentication) varmistetaan, että osapuolet ovat niitä, joita sanovat olevansa. Esimerkiksi sähköisessä kaupankäynnissä ja pankkipalveluissa on aina tärkeää tietää, kuka toinen osapuoli on. Näissä tapauksissa voi liikkua hyvinkin arkaluontoista ja arvokasta tietoa, joten tarvitaan toisen osapuolen ja tietolähteen eli tiedon alkuperän todennusta. Kiistämättömyydellä (deniability) tarkoitetaan sitä, ettei lähettäjä tai vastaanottaja voi kiistää olleensa mukana tapahtumassa, jossa on vaihdettu tietoja. Kiistämättömyys on hyvin tärkeä osa sähköistä kaupankäyntiä, jossa on tärkeä tietää, että myyjä ja ostaja ovat luotettavia. Kiistämättömyys on tietolähteen todennuksen vahva muoto ja se toteutetaan sähköisellä allekirjoituksella. Pääsynvalvonnalla (access control) tarkoitetaan, että käyttäjien pääsyä koneessa olevaan tietoon rajoitetaan ja valvotaan. Pääsynvalvonnalla tarkistetaan, onko osapuolella oikeus palvelun ja tiedon käyttöön, jolloin vain todennetut henkilöt pääsevät käyttämään tietoja. Esimerkiksi yrityksen toimitusjohtajalla on eri oikeudet järjestelmään, kuin oh-

jelmoijalla. Pääsynvalvonnan tavoitteena on osaltaan turvata tiedon luottamuksellisuus ja eheys. (Tietoturvan perusteet, 2005)

2.1 Osa-alueet

Tietoturvallisuus on suuri kokonaisuus, joten se on pilkottu pienempiin osiin. Näin tietoturvallisuutta on huomattavasti helpompi käsitellä. Tietoturvasuunnitelmat voidaan myös rakentaa täysin näiden osioiden pohjalle:

- hallinnollinen turvallisuus
- fyysinen turvallisuus
- henkilöturvallisuus
- tietoaineistoturvallisuus
- ohjelmistoturvallisuus
- laitteistoturvallisuus
- tietoliikenneturvallisuus

Hallinnollisessa turvallisuudessa on kyse siitä, että pyritään varmistamaan tietoturvan kehittäminen ja johtaminen. Se sisältää myös yhteydenpidon eri turvallisuudesta vastaaviin elimiin organisaation sisällä sekä sen ulkopuolella toimiviin viranomaisiin. Yksi tärkeimpiä asioita on lainsäädäntöön liittyvien erilaisten yksityisoikeudellisten sopimusten, kuten lisenssisopimusten ja palvelusopimusten, vaikutusten arviointi organisaation tietoturvakäytäntöihin. (Hakala, Vainio & Vuorinen, 2006, 10-11)

Fyysinen turvallisuus sisältää rakennuksen tilojen ja niihin sijoitettujen laitteiden suojaamisen erilaisilta fyysisiltä uhkilta, kuten murroilta ja ilkivallalta, sekä erilaisilta ympäristöuhkilta, kuten vesi- ja palovahingoilta. Myös mahdolliset sähkö- ja lämmitysjärjestelmien toimintahäiriöt tulee ottaa huomioon. Esimerkiksi palvelintilojen ja tärkeiden tietoliikennelaitteiden fyysiseen suojaukseen tulee kiinnittää erittäin paljon huomiota ja sen tulee olla korkeatasoinen. (Hakala, Vainio & Vuorinen, 2006, 11)

Henkilöturvallisuus tarkoittaa sitä, että tietojärjestelmä täytyy pyrkiä suojaamaan sen käyttäjien aiheuttamilta uhilta. Käyttäjien tekemiä vahinkoja voidaan vähentää (mutta ei poistaa) riittävällä käyttäjien opastuksella ja koulutuksella tietojärjestelmän käytössä. Näitä vahinkoja on mahdollista vähentää antamalla käyttäjille vain ne käyttöoikeudet, jotka he tarvitsevat. Esimerkiksi yrityksen sihteeri ja ohjelmoija eivät tarvitse samoja oikeuksia järjestelmään. Myös tärkeiden käyttäjien taustojen tarkistaminen on

suotavaa, ettei esimerkiksi petoksesta tuomittu henkilö pääse vastaamaan tietojen varmuuskopioinnista tai laskutuksesta. (Ruohonen, 2002, 5)

Tieto on nykyään yksi tärkeimpiä kaupankäynnin kohteita. Se voi sisältää merkittäviä taloudellisia, oikeudellisia ja jopa yhteiskunnallisia arvoja. Tietojen joutuminen luvattomasti ulkopuolisten käyttöön voi johtaa niiden väärinkäyttöön, mistä voi aiheutua yritykselle suuria taloudellisia tappioita. Jotta väärinkäyttö pystytään estämään, on yrityksen jokaisen työntekijälle kerrottava yrityksen tietojen todellinen arvo. Näin työntekijät voivat käsitellä ja suojata tietoja niiden arvon mukaisesti. Tietoaineistoturvallisuudessa tarkastellaan näitä asioita. (Miettinen, 2002, 132)

Ohjelmistoturvallisuudessa on kyse tietojärjestelmässä käytettyjen ohjelmien suojaamisesta luvattomalta käytöltä ja käytettävien ohjelmien lisenssien ylläpitämisestä. Esimerkiksi käytettävien ohjelmien lisenssien ylläpito on tärkeää sen takia, että yritykselle ei tule ongelmia, mikäli viranomaiset päättäisivät jostain syystä tutkia tietojärjestelmän laittomien ohjelmien varalta, niin myös siksi, ettei jokin tietojärjestelmän tärkeä ohjelma lopettaisi toimintaansa lisenssien käyttöajan loputtua. Ohjelman toimimattomuus voi aiheuttaa yritykselle suuriakin tappioita. (Ruohonen, 2002, 4)

Laitteistoturvallisuudessa on kyse tietojärjestelmään kytkettyjen laitteiden - eli tietokoneiden, palomuurien ja palvelinten - suojaamisesta. Laitteistoturvallisuuteen kuuluvat myös laitteiston tarkoituksenmukainen mitoitus, toiminnan testaus, huollon järjestäminen sekä varautuminen laitteiden kulumiseen ja vanhentumiseen. Laitteistoturvallisuus sisältää myös laitteiden käytöstä aiheutuvien vaaratekijöiden, kuten sähköiskun tai muun loukkaantumisvaaran, arvioinnin ja minimoinnin. (Hakala, Vainio & Vuorinen, 2006, 12)

Tietoliikenneturvallisuudessa on kyse tietojärjestelmässä käytettävien tiedonsiirtoratkaisujen, kuten lähiverkkojen suojaamisesta. Tietoliikenneturvallisuutta voidaan parantaa eristämällä tietojärjestelmän verkko muista verkoista palomuureilla ja salaamalla järjestelmän ulkopuolisten verkkojen kautta kulkeva tietoliikenne esimerkiksi VPN-verkkojen avulla. (Ruohonen, 2002, 4)

Periaatteessa mukaan voidaan liittää myös käyttöturvallisuus, joka tarkoittaa sitä, että tietojärjestelmää käytetään turvallisesti. Siihen sisältyvät myös käytöstä aiheutuvat riskit ja niihin varautuminen. Käytön turvallisuus kuitenkin jo sisältyy maalaisjärjellä ajateltuna kaikkiin edellä mainittuihin osa-alueisiin.

2.2 IT-ympäristöön kohdistuvat uhat

Yrityksille voi tulla eteen monenlaisia IT-ympäristöön kohdistuvia uhkia. Yrityksen palvelimen voi hajota, työntekijän kannettava tietokone varastetaan tai vaikka alueen läpi kulkeva joki tulvii keväällä ja aiheuttaa yrityksen tiloissa pahan vesivahingon. Uhkien taustalla voivat olla käyttäjien tekemät virheet. Nykyajan tekniikkakaan ei ole täysin varmaa, joten tekniikan pettäminenkin on yksi mahdollisista uhkista. Internetin yleinen käyttö on myös tuonut oman lisänsä tähän kokonaisuuteen. Internetin kautta leviävät virukset, haitta-ohjelmat ja troijalaiset. Jopa hakkerit voivat pahimmassa tapauksessa päästä Internetin kautta käsiksi yrityksen tietoihin. Myös harvinaisemmat luonnonmullistukset, kuten maanjäristykset voivat aiheuttaa suuria ongelmia yritykselle. Tällaisiin asioihin ei välttämättä osata varautua millään tavalla.

2.2.1 Työntekijät

Suurin osa uhkista johtuu valitettavasti käyttäjien (työntekijöiden) tekemistä virheistä. Virheet voivat johtua käyttäjien huolimattomuudesta tai yksinkertaisesti osaamattomuudesta. Ollessani töissä tietokoneiden huoltoon erikoistuneessa yrityksessä eteeni osui monenlaisia käyttäjien aiheuttamia ongelmia: Tietokone hajoaa, koska käyttäjältä on kaatunut kahvia tietokoneen päälle. Huonot ja helpot salasanat kuuluvat myös käyttäjien aiheuttamiin uhkiin. Käyttäjä voi myös tiedon puutteen takia avata sähköpostiin tulleen saastuneen liitetiedoston. Tätä uhkaa pystytään pienentämään pitämällä koulutuksia ja valistamalla käyttäjiä vaaroista.

2.2.2 Uudet tietokoneet

Yrityksille tulee jossain vaiheessa eteen uusien tietokoneiden hankinta, jolloin vanhat koneet annetaan käytettäväksi muuhun tarkoitukseen tai yksinkertaisesti viedään kierrätykseen. Uusien tietokoneiden hankinnan ensimmäinen askel on se, että mitä tehdään vanhoille tietokoneille. Tietokoneiden kiintolevyt pitää muistaa tyhjentää kunnolla ennen kuin ne laitetaan kiertoon. Pelkkä levyn formatointi tai poista-komento ei tyhjennä levyä kokonaan. Paras tapa on vaihtaa koneeseen uusi kiintolevy ja tuhota vanha levy perusteellisesti. Uusiin tietokoneisiin täytyy muistaa ladata käyttöjärjestelmän uusimmat päivitykset ja asentaa virustorjuntaohjelmisto. Uusi tietokone on hyvin altis viruksille. Henkilökohtaisiin kokemuksiin perustuen suojaamaton tietokone voi saastua pahimmassa tapauksessa heti, kun se on yhdistetty Internetiin.

2.2.3 Järjestelmäkaatumiset ja odottamattomat tapahtumat

Vaikka nykyajan tekniikka onkin kehittynyttä, se ei silti takaa ongelmatonta toimintaa. Tietokoneen käyttöjärjestelmä voi mennä sekaisin ja aiheuttaa käyttökatkoksen tai pahimmassa tapauksessa tietojen menetyksen. Myös erilaiset onnettomuudet, kuten tulvat, maanjäristykset, tulipalot tai vesivahingot voivat aiheuttaa vahinkoa yritykselle. Mikäli edellä mainittuihin onnettomuuksiin ei olla millään tavalla varauduttu, seurauksena voi olla tärkeiden tietojen häviäminen ja suuret rahalliset menetykset. Näitä riskejä ei kannata jättää huomioimatta, vaikka niiden sattuminen omalle kohdalle voi vaikuttaa hyvin epätodennäköiseltä. (Symantec, 2007, 17)

2.2.4 Varkaus

Kannettavia käytetään nykyään paljon niiden helpon liikuteltavuuden takia. Liikuteltavuus altistaa kannettavat kuitenkin varkauksille. Kannettavien tietokoneiden rahallinen arvo on yleensä kohtuullisen suuri, joten se houkuttelee varkaita. Varkauden sattuessa voi tapahtua suurikin vahinko, jos tietokone on sisältänyt tärkeitä tiedostoja. Etenkään julkisilla paikoilla kannettavaa tietokonetta ei saa jättää ilman valvontaa. Varkaille kelpaavat myös kannettavat muistivälineet, kuten USB- muistitikut. (Symantec, 2007, 17)

2.2.5 Suunnatut hyökkäykset

Suunnatut hyökkäykset ovat pahimpia uhkia, mitä yrityksille eteen voi tulla. Nämä hyökkäykset voivat pahimmassa tapauksessa lamauttaa yrityksen toiminnan kokonaan. Yleensä suoraan suunnatut hyökkäykset kohdistuvat suuriin ja tunnettuihin yrityksiin. Mutta tämä ei tarkoita sitä, että pienemmät yritykset ovat täysin turvassa. Nykyään suurimmalla osalla yrityksistä yritysten omat tietoliikenneverkot ovat yhteydessä Internetiin, joka antaa mahdollisuuden hyökkäykseen. Suunnattua hyökkäystä ei tarvitse kohdistaa suoraan yritystä vastaan. Vuosia takaperin hakkerit murtautuivat huonosti suojattuihin järjestelmiin ja lähettivät niihin matoja tai viruksia puhtaasti vain näyttääkseen, että se on mahdollista. Nykyaikana kuitenkin näiden useimpien Internet-hyökkäysten syynä on saada jonkunlaista taloudellista hyötyä, mutta kiusantekokin on valitettavan yleistä. Esille on myös tullut tapauksia, joissa yrityksiin on kohdistettu suoraa kiristystäkin. Tekijät voivat esimerkiksi uhata ylikuormittavansa Internet-sivustoa niin, että sen toimintaa hidastuu huomattavasti tai lopettaa kokonaan toimintansa. Sivuston ylikuormitus tapahtuu yleensä siten, että huonosti suojatut tai kokonaan suojaamattomat tietokoneet saavat tartunnan ja ne muodostavat suuren hyök-

käysverkon. Tämä tapahtuu yleensä vielä siten, että tietokoneen käyttäjillä ei ole asiasta mitään tietoa. Näin ollen tällainen ongelma voi tulla eteen ihan kenelle vaan. (Symantec, 2007, 19)

2.2.6 Virukset ja madot

Tietokonevirus on tavallisen näköinen sovellus, joka pystyy saastuttamaan muita ohjelmia tai tiedostoja muuttamalla niitä siten, että itse virusohjelma kopioituu niihin. Käytännössä voidaan todeta, että virukset ovat ohjelmia, joilla on kyky monistaa itseään. Yleensä virukset saastuttavat käyttöjärjestelmän tiedostoja, joiden saastuminen aiheuttaa koneelle paljon häiriöitä ja ongelmia. Virukset voivat pahimmassa tapauksessa sekoittaa tietokoneen toiminnan täysin. Mikäli saastunut tietokone on yhteydessä lähiverkon kautta muihin koneisiin, virus voi levitä joka puolelle. Nykyään on tullut ilmi myös sellaisia viruksia, jotka siirtyvät koneelta toiselle USB- muistien välityksellä. Kun muistin laittaa koneeseen kiinni, virus siirtyy automaattisesti tietokoneelle ja alkaa tehdä tuhojaan. Tällaisten virusten poistaminen on erittäin työlästä ja se voi käydä yritykselle kalliiksi. (Symantec, 2007)

Madot ovat viruksenkaltaisia haittaohjelmia, jotka leviävät verkon tai Internetin kautta muihin tietokoneisiin. Matojen vahinko perustuu siihen, että ne tekevät itsestään itsenäisiä kopioita ja näin ylikuormittavat järjestelmää. Matoja voi joskus olla niin paljon, että koko Internet yhteys voi hidastua. (F-Secure, 2010b.)

Tietokoneessa käytössä olevalla käyttöjärjestelmällä on merkitystä, kuinka paljon viruksista on haittaa. Ylivoimaisesti eniten viruksia on Microsoftin kehittämille Windows-käyttöjärjestelmille. Tällä hetkellä on käytössä vielä kolmea eri Windows-käyttöjärjestelmää, joista opinnäytetyön tekijällä on henkilökohtaista kokemusta: Windows XP, Windows Vista ja Windows 7. Näistä XP on vanhin ja se on päivittämättömänä erittäin huonosti suojattu. Kun muistaa pitää automaattiset päivitykset päällä ja käytössä on ajan tasalla oleva virusturva ja palomuuri, ei pitäisi olla kovin suurta hätää. Windows Vista on eräänlainen väliinputoaja. Sen tietoturvaominaisuudet eivät ole parhaasta päästä ja se on hidas. Näin ollen monet käyttäjät ovat hypänneet yli Vistasta ja siirtyneet uusimpaan versioon, eli Windows 7:aan. Tosin nykyään vielä käytetään hyvinkin laajasti XP:tä. Linux- ja Macintosh käyttöjärjestelmän käyttäjät ovat paremmassa turvassa viruksien suhteen, mutta niillekin on alkanut tulla viruksia.

2.2.7 Phishing

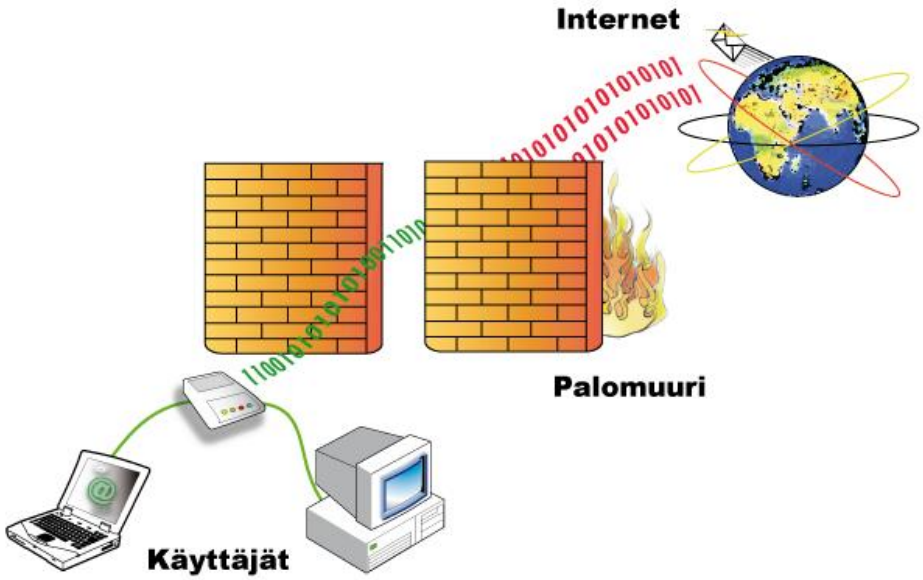
Phishing tarkoittaa tietojen kalastelua haitallisessa tarkoituksessa. Tietojen kalastelua ovat muun muassa sähköpostiviestit, joissa yritetään pyytää luottamuksellisia tietoja, kuten luottokortin numeroa tai tilinumeroa. Lähetetyt viestit voivat yleensä olla hyvinkin aidon tuntuisia, mutta yleensä joku asia paljastaa huijauksen. Muun muassa lähettäjän osoite on yleensä outo ja viestit voivat sisältää huomattavia kirjoitusvirheitä. Muista aina se, että pankit eivät koskaan kysy tili- tai luottotietoja sähköpostin kautta! (Symantec, 2007, 22)

3 TIETOTURVARATKAISUT

Tietokoneiden suojaksi on kehitetty erilaisia fyysisiä laitteita ja ohjelmia, joilla saadaan kone pidettyä puhtaana viruksista, tunkeutujista ja haittaohjelmista. Ylivoimaisesti tunnetuimmat termit ovat palomuuri ja virustorjunta.

3.1 Palomuuri

Palomuuri (firewall) on tietoturvan yksi tunnistetuimpia termejä. Palomuurin toiminta perustuu siihen, että se sulkee tietokoneesta sellaiset portit, jotka eivät ole käytössä. Kuvassa 1. näytetään palomuurin toiminta yksinkertaistettuna. Kun tietokone on liitetty verkkoon, siinä voi olla avoinna jopa tuhansia fyysisiä ja virtuaalisia portteja, joiden kautta haitalliset ohjelmat voivat päästä tietokoneelle. Nykyaikainen palomuuri pystyy sulkemaan suurimman osan näistä porteista. Palomuurin tärkein tehtävä on tarkkailla sisään tulevaa liikennettä ja pitää ylimääräiset tunkeilijat ja uhat poissa. Palomuuria voidaan myös tarvittaessa käyttää toisinkin päin. Sillä voidaan rajoittaa käyttäjien tietoliikennettä ulospäin. Palomuuri on pakollinen, jos käytössä on jonkinlainen Internet -yhteys. Olen nähnyt tietokoneen saastuvan samalla hetkellä kun se sai yhteyden Internetiin, kun sitä ei ollut suojattu palomuurilla.



Kuva 1. Yksinkertaistettu kuva palomuurin toiminnasta. (Wikimedia, 2005)

3.1.1 Palomuurin tyypit

Palomuuri voi olla joko laite- tai ohjelmistopohjainen. Ohjelmistopohjainen palomuuri voidaan asentaa tavalliseen tietokoneeseen, jonka kautta sitä käytetään. Nykyaikana palomuuriohjelmistot voivat sisältää muun muassa virustorjunnan ja sähköpostisuodatuksen. Laitteistopohjaiset palomuurit ovat erillisiä laitteita, joita käytetään suurempien verkkojen yhteydessä. Kotikäyttäjälle laitteistopohjainen palomuuri on yleensä turhan kallis hankkia. Normaalia laajakaistayhteyttä käyttäville on järkevää hankkia laajakaistamodeemi, joka sisältää palomuuriominaisuuden. Markkinoilla on tarjolla myös palomuureja, jotka sisältävät paljon hyödyllisiä toimintoja. Laitteet voivat sisältää sisällön suodatuksen, VPN:n, virusturvan ja tietomurtojen havainnoinnin. (Symantec, 2007, 46 - 47)

3.1.2 Palomuurin säännöt ja seuranta

Säännöt ovat palomuurin tärkein osa, sillä palomuuri on vain niin turvallinen kuin siihen asennetut säännöt. Palomuurin säännöille voidaan asettaa nämä tavoitteet: Sääntöjä tulee liiallisen monimutkaisuuden välttämiseksi olla mahdollisimman vähän. Sääntöjen tulee rajoittaa liikennettä mahdollisimman paljon. Myös suojatusta verkosta lähtevää liikennettä tulisi rajoittaa verkon tietokoneille päässeiden troijalaisten varalta. Säännöt on asetettava siten, etteivät ne estä käyttäjien normaalia työskentelyä. (Ruohonen, 2002, 66)

Palomuurin toimintaa tulee seurata säännöllisin väliajoin. Palomuurit luovat koko ajan loki-tiedostoa, josta näkyvät kaikki palomuuriin tulleet yhteyden muodostusyritykset, sallitut yhteydet ja blokatut yhteydet. Loki-tiedostoa tutkimalla on mahdollista saada jonkinlainen käsitys yrityksen tietoturvasta. (Symantec, 2007, 47)

3.2 Virustorjunta

Nykyaikana Internet on täynnä viruksia. Niitä on liikkeellä jopa satoja tuhansia, joten hyvin suurella todennäköisyydellä jokainen tietokonetta käyttänyt joutuu jossakin vaiheessa tekemisiin virusten kanssa. Virukset ja haittaohjelmat voivat levitä niin monella eri tavalla, että virustorjuntaohjelmisto on pakollinen, vaikka tietokone ei olisikaan liitetty Internetiin. Ajan tasalle päivitetty virustorjuntaohjelmisto auttaa tiedostojen säilyttämisessä. Virukset voivat saastuttaa koneella olevia tiedostoja ja niitä ei välttämättä pysty puhdistamaan. Näin ollen tärkeistäkin tiedostoista voi tulla käyttökelvottomia. (Symantec, 2007, 47-48)

Virustorjuntaohjelmat tutkivat tietokoneen kiintolevyltä tiedostoja, niin sanottuja saastuneita tiedostoja, jotka voivat aiheuttaa tietokoneelle ongelmia. Virustorjuntaohjelmiston toiminta perustuu siihen, että se sisältää erilaisten haittaohjelmien ja virusten tunnistetiedot, joiden perusteella se etsii saastuneita tiedostoja. Virustorjuntaohjelmia täytyy päivittää säännöllisesti, koska uusia viruksia ilmestyy koko ajan ja päivittämätön ohjelma ei tunnista uusia viruksia. Henkilökohtaisen kokemuksen perusteella kotikäyttäjälle parhaimpia virustorjuntaohjelmia ovat virustorjuntaohjelman ja ohjelmallisen palomuurin yhdistelmät, jotka suodattavat hyvin viruksia ja haitalliset yhteysyritykset.

4 KÄYTTÄJIEN TIETOTURVA

Yritysten tietoturvallisuus on usein tekniseltä osaltaan hyvässä kunnossa, mutta käyttäjien osaaminen voi tuottaa paljon ongelmia. Käyttäjät voivat jossakin vaiheessa tuudittautua turvallisuuden tunteeseen, mikä on suuri virhe. Käyttäjiä pitäisi muistuttaa riittävän usein tietoturvan tärkeydestä. Valitettavasti suurin osa yrityksien tietoturvaongelmista johtuu edelleen käyttäjien tekemistä virheistä. Kaikkia virheitä ei voi millään kitkeä pois, koska osa asioista sattuu vahingossa. Oikeanlaisilla toimintaohjeilla on kuitenkin mahdollista vähentää vahinkojen määrää.

Kaikille työntekijöille olisi hyvä tehdä selväksi oma vastuu työtehtäviin liittyvästä tietoturvasta. Näin työntekijä ymmärtää, kuinka hänen tulee toimia. Uusien työntekijöiden kohdalla tämä on erityisen tärkeää. Uusille työntekijöille koulutetaan heti ensimmäisenä tietoturvaan liittyvät käytänteet ja opetetaan toimimaan niiden mukaan. Uusien työntekijöiden palkkaamisen kohdalla kannattaa usein selvittää työntekijöiden taustat. Etenkin jos työtehtävä on hyvin salainen tai siinä toimitaan luottamuksellisten asioiden, kuten valuutan ja henkilötietojen kanssa. (Ruohonen, 2002, 5)

Käyttäjien tietoturvaan tärkeästi liittyvä asia on myös se, että kaikille työntekijöille ei tarvitse antaa samoja käyttö- ja kulkuoikeuksia. Esimerkiksi yrityksen sihteerin ei tarvitse päästä käsiksi palvelimeen liittyviin asiakirjoihin. Näin pystytään karsimaan ainakin osa mahdollisista riskeistä.

4.1 Salasanat

Salasanoja käytetään nykyään joka paikassa. Valitettavasti käytettävät salasanat ovat aivan liian helppoja ja yksinkertaisia. Harmillista ja sinällään huvittavaa on se, että maailman yleisimmät salasanat ovat "password" ja "123456". Salasana ei saa kuitenkaan olla liian vaikea. Salasana on silloin liian vaikea, jos sen kirjoittamiseen tai muistamiseen joutuu kuluttamaan paljon aikaa. Salasanat kannattaa vaihtaa myös usein. Esimerkiksi kolmekymmentä tai kuusikymmentä päivää on hyvä vaihtoväli. (Vance, 2010)

4.2 Hyvän salasanan vaatimukset

Koska salasanat ovat yleensä ainoa suojaus, joka estää ketä tahansa ulkopuolista kirjautumasta järjestelmään käyttäjätunnuksella, tulee salasanat valita siten, että niiden murtaminen on mahdollisimman vaikeaa. Hyvälle salasanalle voidaan asettaa seuraavat vaatimukset: (Ruohonen, 2002, 151)

- Salasanan tulee olla riittävän pitkä (vähintään 6-8 merkkiä)
- Salasanassa tulee käyttää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä (?#%¤!)
- Salasana ei saa löytyä minkään kielen sanakirjasta
- Salasana ei saa olla johdettu käyttäjätunnuksesta (oikein- tai väärinpäin)
- Salasana ei saa olla jokin käyttäjään helposti yhdistettävä asia, kuten harrastukset, mietelauseet, nimet, syntymäpäivät jne.
- Salasana vaihtuu välillä

Käyttäjillä voi olla usein monia eri ohjelmistojen, tietokoneiden ja järjestelmien salasanoja muistettavana. Näissä kaikissa järjestelmissä ei saa käyttää missään nimessä samaa salasanaa. Hyvämuistisella käyttäjälläkin voi jossain vaiheessa tulla ongelmia kaikkien salasanojen kanssa. Paras tapa on hankkia salasanojen hallintaohjelma tietokoneelle, minne voidaan tallentaa salasanoja. Tämä ohjelma on suojattu salasanalla, joten yhdellä salasanalla pääsee tarkastamaan salasanat, jotka ovat päässeet unohtumaan. Tällä tavoin ei tarvitse muistaa kaikkia salasanoja, eikä kirjoittaa niitä ylös paperille.

4.3 Koulutus

Yrityksien kannattaa pyrkiä ennaltaehkäisemään työntekijöistä aiheutuvia tahallisia tai tahattomia vahinkoja. Kouluttaminen ja ohjeistaminen auttavat työntekijöitä toimimaan oikein erilaisissa vaikeissa tilanteissa. Yrityksen kannattaa suunnitella myös eri työprosessit siten, että niissä on mahdollista huomata virheet ennakolta.

Käyttäjille tulee pitää riittävän monta kertaa vuodessa koulutuksia, jossa käydään läpi tietoturvallisuuteen liittyviä uusia käytänteitä ja muistutetaan vanhoista asioista. Kaikki edellisissä koulutuksissa käydyt asiat eivät välttämättä jää riittävän pitkäksi aikaa muistiin, vaan ne unohtuvat jossakin vaiheessa. Käyttäjille pitää myös pystyä sisäistämään se ajatus, että tietoturvan ylläpito on tärkeää ja sen onnistuminen alkaa käyttäjien omista teoista ja toimimisesta.

Voidaankin todeta, että tietoturvakäytännöstä ei ole mitään hyötyä, jos se on erittäin hienosti ja hyvin laadittu tai kattava, mutta käyttäjät eivät ymmärrä kuinka sitä tulee soveltaa käytännössä. (Symantec, 2007, 33)

4.4 Kulunvalvonta

Kulunvalvonnan perusajatuksena on valvoa ihmisten liikkumista yrityksen tiloissa ja piha-alueilla. Valvonnan tulee kattaa sekä oman henkilöstön että yrityksen tiloissa liikkuvat vierailijat ja ulkopuoliset työntekijät. Ammattimaisesti toteutettu kulunvalvonta perustuu yleensä sähköisten lukitusten- ja kulkukorttien käyttöön, joiden hallinta voidaan tehdä helposti tietokoneen avulla. (Miettinen, 2002, 98)

5 ETÄTYÖSKENTELY

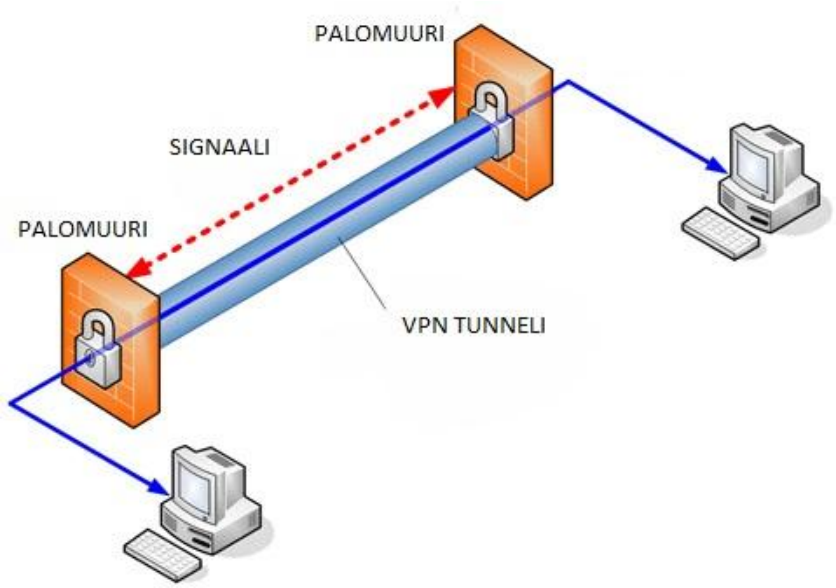
Nykyajan erilaiset mobiiliratkaisut lisäävät työntekijöille paljon erilaisia mahdollisuuksia työntekoon, mutta huono puoli on se, että ne tuovat mukanaan uusia riskejä. Mobiililaitteet antavat mahdollisuuden työskennellä missä ja milloin tahansa, mutta samalla liiketoimintaan liittyvät kriittiset tiedot joutuvat toimiston ulkopuolelle ja ulkona ne eivät ole niin hyvin suojassa. (Symantec, 2007)

Etätyöskentely on yksi tekniikan kehittymisen myötä tulleita helpotuksia työn tekemiseen. Tämä helpotus aiheuttaa kuitenkin paljon lisätyötä tietoturvan ylläpitoon. Etätyöntekijät haluavat yleensä muodostaa yhteyden yrityksen verkkoon, jotta pääsevät käsiksi yrityksen tietoihin. Yhteydenmuodostus on ensimmäinen tärkeä asia. Käytettävässä tietokoneessa tulee myös olla päivitykset, virustorjunta ja palomuuri ajan tasalle päivitettynä. (Symantec, 2007)

5.1 VPN

VPN-verkko (Virtual Private Network) on julkisen verkon sisällä toimiva suojattu verkko. Tarkoituksena on käyttää jo olemassa olevaa julkista verkkoa siten, että vain suojattuun verkkoon kuuluvat tietokoneet voivat lähettää ja vastaanottaa suojattuun verkkoon osoitettuja viestejä Tämä pienentää kustannuksia, kun suojattua verkkoa ei tarvitse erikseen rakentaa. (Ruohonen, 2002, 95)

Uudet ja monipuoliset fyysiset palomuurit sisältävät VPN-ominaisuuden, jonka avulla on mahdollista luoda virtuaalinen verkko. Kuten kuvasta 2 voidaan huomata, VPN on periaatteeltaan varsin yksinkertainen. Se luo niin sanotun suojatun tunnelin, jota voivat käyttää vain suojattuun verkkoon kirjautuneet. (Ferguson, P. & Huston, G. 1998)



Kuva. 2 VPN yksinkertaisimmillaan (ZAPware, 2011, muokattu)

5.2 WLAN

WLAN (Wireless Network) tarkoittaa langatonta verkkoa. Langattomien verkkojen suosio on kasvanut viime vuosina räjähdysmäisesti. WLAN helpottaa etätyötä huomattavasti, kun tietokoneen ei tarvitse olla kytkettynä verkkojohtoon, päästäkseen sillä yrityksen verkkoon. Langattomia verkkoja on käytössä kaikkialla; lentokentillä, rautatieasemilla ja jopa ravintoloissa. Perusasetuksiltaan langattomat verkot ovat yleensä suojaamattomia, mikä tarkoittaa sitä että kuka tahansa verkon löytänyt voi siihen liittyä. Tämän takia verkko tulee suojata jonkunlaisella salauksella. Kun käytössä ei ole minkäänlaista suojausta, kuka tahansa voi liittyä langattomaan verkkoon ja käyttää sitä. Käyttäjä voi mahdollisesti päästä käsiksi jaettuihin tiedostoihin ja resursseihin (Symantec, 2007, 26)

5.3 Kannettavat tietokoneet

Kevyet ja helposti mukana kulkevat kannettavat tietokoneet ovat ohittaneet suosiossa painavat ja isokokoiset pöytäkoneet. Tehoero näiden kahden konetyypin välillä on hyvin pieni. Kannettavissa tietokoneissa on kuitenkin myös huonot puolensa: Helpon liikuteltavuuden myötä ne ovat myös helposti varastettavissa. Erittäin tärkeä asia kannettavien tietokoneiden kohdalla on se, että ne tulee aina suojata salasanalla. Kannettavia tietokoneita käytetään yleensä langattomien verkkojen kanssa, joten niihin tulee hankkia hyvä virustorjunta- ja palomuuriohjelmisto. Mikäli käytetään suo-

jaamattomia verkkoja, kuka tahansa voi helposti tunkeutua tietokoneelle, jos minkäänlaista palomuuria ei ole käytössä. Automaattinen vapaaseen langattomaan verkkoon kytkeytyminen kannattaa ottaa pois päältä, ettei sieltä tule mahdollisia viruksia. (Symantec, 2007)

5.4 Älypuhelimet

Puhelimia eivät ole enää tehty pelkästään puhumista varten. Ne ovat käytännössä pienikokoisia tietokoneita, joilla on mahdollista tehdä etätyötä. Älypuhelimet ovat kannettavien tietokoneiden tavoin alttiita joutua varastetuiksi. Näin ollen puhelimet kannattaa suojata ohjelmistolla, jolla puhelin voidaan lukita Internetin kautta. Käytännössä älypuhelimen käyttöön liittyvät samanlaiset säännöt, kuin kannettaviin tietokoneisiinkin. Nykyään virukset ja haittaohjelmat ovat levinneet jo puhelimiinkin, joten niihinkin kannattaa hankkia virustorjuntaohjelmisto; esimerkiksi F-Secure tai McAfee. Kuten kannettavissa tietokoneissakin, älypuhelimien verkon käyttöä kannattaa rajoittaa ja verkkoihin automaattisesti liittyminen kannattaa ottaa pois päältä. Näin käyttäjä liittyy verkkoon vain halutessaan. Puhelimet tulee myös suojata kunnollisella PIN-koodilla. Yleensä alkuperäinen PIN-koodi on joko 0000 tai 1234. Se on aivan liian helppo arvata, joten se kannattaa vaihtaa. Puhelimesta kannattaa ottaa myös varmuuskopioita säännöllisin väliajoin, koska ne ovat uutta tekniikkaa ja uusi tekniikka on nykyään vielä harmillisen lyhytikäistä. (F-Secure, 2010a.)

6 SUOJAUTUMINEN TIETOJEN HÄVIÄMISTÄ VASTAAN

Tärkeiden tietojen menettäminen tai häviäminen voi koitua yrityksen kohtalolle kalliiksi. Tärkeimpien liikesalaisuuksien vuotaminen kilpailijoille voi sysätä yrityksen jopa konkurssiin. Tästä syystä yritysten tulee tehdä kaikki mahdollinen tietojen suojaamiseksi. Tietojen häviämistä voidaan vähentää varmuuskopioinnilla ja käyttämällä tietoliikenne- ja tietokonelaitteiston kanssa UPS-laitetta.

6.1 Varmuuskopiointi

Varmuuskopioinnilla voidaan luoda riittävä tietoturvataso ja sen myötä voidaan taata yrityksen tietojen saatavuus. Varmuuskopiointi on mahdollista toteuttaa joko ohjelmistoilla tai laitteilla. Varmuuskopioinnilla voidaan kopioida talteen käyttäjän tärkeimmät tiedostot, ohjelmat tai koko kiintolevyn sisältö. Pelkkä varmuuskopiointi ei riitä, vaan sen lisäksi on oltava nopea tapa palauttaa vanhat tiedostot takaisin käyttöön jotta työt saadaan jatkumaan. Mahdollisen käyttökatkoksen kulut voivat helposti ylittää tehokkaan ja toimivan varmuuskopiointityökalun kulut. (Symantec 2007, 37)

Varmuuskopioinnin perusperiaatteisiin kuuluu se, että varmuuskopiointi tulee olla jatkuvaa. Varmuuskopioiden palauttamista tulee myös testata säännöllisin väliajoin. Testaamalla varmistetaan varmuuskopioiden toimivuus. Tallessa olevista tiedostoista kun ei ole mitään hyötyä, jos niihin ei päästä käsiksi. Varmuuskopioista voidaan ajatella myös siten, että palautus on aina vain niin hyvä, kuin alkuperäinen varmuuskopio. Vähemmän tärkeissä asioissa varmuuskopiointi voidaan suorittaa esimerkiksi kerran päivässä, mutta tärkeissä asioissa, kuten sähköposti- ja tiedostopalvelimissa varmuuskopioinnin tulee olla jatkuvaa. (Drake, 2007)

6.1.1 Kannettavat tallennusvälineet

Yksinkertaisimmillaan varmuuskopiointi voidaan hoitaa käyttämällä erilaisia kannettavia tallennusvälineitä. Esimerkiksi USB-väylässä toimivat muistitikut tai ulkoiset kiintolevyt käyvät varmuuskopiointiin hyvin. Kannettavat tallennusvälineet sopivat hyvin pienille yrityksille, joilla on vähän varmuuskopioitavaa. Kannettavat tallennusvälineet soveltuvat hyvin käytettäväksi kannettavien tietokoneiden kanssa, koska kannettavaa tietokonetta ei aina saada liitettyä yrityksen yhteiseen verkkoon. (Drake, 2007)

6.1.2 Nauhavarmistus

Nauhavarmistusasemat ovat yleisimpiä varmuuskopiointityökaluja. Nauhavarmistusasemat toimivat samalla tavalla kuin kasettisoittimet. Tieto tallentuu nauhalle, joten jos siitä halutaan etsiä tiettyä tiedostoa, niin sitä joutuu kelaamaan sopivaan kohtaan. Nauhavarmistusasemat alkavat olla jo vanhentunutta tekniikkaa, mutta niitä voidaan kuitenkin vielä käyttää, mikäli kopioitavien tietojen määrä ei ole suuri. (Drake, 2007)

6.1.3 Online-varmuuskopiointi

Paras paikka varmuuskopioiden säilyttämiseen on aivan jossain muualla kuin alkuperäisten kopioiden luona. Nykyiset tiedonsiirtonopeudet mahdollistavat Online-varmuuskopioinnin, joka mahdollistaa varmuuskopioiden tallentamisen vaikka toiselle puolelle maapalloa. Online-varmuuskopioinnissa on kyse palvelusta, jonka avulla varmuuskopiot voidaan tallentaa turvallisesti verkossa olevalla palvelimelle. Palvelu toimii yleensä tietokoneelle asennettavan ohjelmiston kautta, joka tekee kopioinnin haluttuun aikaan. Ohjelma muuttaa tiedostot suojattuun muotoon ja lähettää tiedostot palvelimelle. (Drake, 2007)

6.1.4 RAID

RAID (Redundant Array of Independent Disks) on tekniikka, jolla tietokoneiden vikasietoisuutta voidaan parantaa. Yksinkertaisesti ilmaistuna RAID-tekniikassa käytetään useita erillisiä kiintolevyjä, jotka yhdistetään yhdeksi loogiseksi levyksi. Tekniikkaa käytetään usein virheettömyyttä vaativissa laitteistoissa, kuten palvelimissa. RAID voidaan toteuttaa monella eri tavalla, mutta yleisimpiä tapoja on kolme: RAID0, RAID1 ja RAID5. Tekniikan käyttäminen ei pelkästään paranna levyjen vikasietoisuutta, vaan se voi myös parantaa suorituskykyä. RAID0 on yksinkertaisin käytettävistä tekniikoista. Tämä tekniikka ei tarjoa parempaa tietojen turvaa, joten sitä ei käsitellä sen suuremmin. (Patterson, D.; Gibson, G. & Katz, R. 1988)

RAID1 eli peilaus on yleisesti käytetty tekniikka, jossa käytössä on kaksi (tai useampi) kiintolevyä, joihin tallennetaan samat tiedot. Näin ollen toisen levyn rikkoontuessa kaikki tiedostot säilyvät tallessa. Tätä tekniikka voi käyttää jo hyvin yhden tietokoneen ja pienen tiedostomäärän varmuuskopiointiin. RAID1- tekniikka myös nopeuttaa kiintolevyjen lukunopeutta. (Diamantis, C. & Yamamura, Y. 2008)

RAID5 on edellä mainittuihin tekniikoihin verrattuna vielä monipuolisempi. Tässä käytössä voi olla vaikka viisi kiintolevyä, joista mikä tahansa voi hajota ilman, että tiedostoja häviää. Tätä tekniikkaa ei kannata käyttää pienitehoisilla tietokoneilla, koska se vaatii paljon tehoja. RAID5:sta on kehitetty vielä uudempi versio, joka kulkee nimellä RAID6. Se toimii samalla tavalla kun RAID5, mutta siitä voi hajota kaksi kiintolevyä yhtä aikaa ilman, että tiedostot häviävät. (Diamantis, C. & Yamamura, Y. 2008)

Suuria tiedostomääriä sisältävissä palvelimissa voidaan käyttää myös Hot swap-järjestelmää, joka mahdollistaa rikkoutuneen levyn vaihtamisen lennosta ilman, että palvelinta tarvitsee käynnistää uudelleen. Kun uuden levyn asettaa takaisin, RAID-järjestelmä rakentaa koko levykuvan levylle uudestaan. (Diamantis, C. & Yamamura, Y. 2008)

6.1.5 NAS

NAS (Network attached storage) tarkoittaa verkkotallennusta. Se on tallennusjärjestelmä, joka on kytketty suoraan verkkoon ja se hoitaa tallennuksen suoraan verkon kautta. Etenkin pienemmissä yrityksissä, jossa ei ole useita tietokoneita, on NAS oiva vaihtoehto. Monissa tallennuskapasiteetiltaan suurissa ulkoisissa kiintolevyissä on NA -ominaisuus mukana. (Drake, 2007)

6.2 UPS

UPS (Uninterrupted Power Supply) on laite, joka suojaa tietokoneita ja palvelimia virtakatkoksilta. Kaikkien palvelimien yhteyteen tulisi asentaa UPS. UPS-laitteen toimintaperiaate on varsin yksinkertainen. Laite sisältää akun tai useampia akkuja, joista se syöttää virtaa tietokoneelle mahdollisen virtakatkon tapahtuessa. Pienimmissä UPS- järjestelmissä virtaa riittää laitteille korkeintaan 30 minuutiksi. Se on kuitenkin riittävä aika, että järjestelmä voidaan sulkea hallitusti ilman tiedostojen menettämistä. UPS-järjestelmien asennus on yleensä varsin helppoa. Suojattavien laitteiden sähköjohdot kytketään UPS-laitteeseen kiinni ja tietokoneelle asennetaan laitteiston hallintaohjelma, jonka avulla voidaan seurata toimintaa ja tehdä asetuksiin muutoksia. (Pacific Gas and Electric Company, 2000)

7 TIETOJEN SÄILYTTÄMINEN JA HÄVITTÄMINEN

Tietoaineiston säilyttäminen turvallisesti on yksi tietoturvan tärkeimpiä ja keskeisimpiä asioita. Sähköisessä muodossa olevista tiedostoista muistetaan yleensä ottaa varmuuskopiot, mutta normaaleihin asiakirjoihin ei huomata kiinnittää huomiota. Niitä lojuu pöydillä kaikkien luettavana ja varastettavana. Toinen valitettavan usein vähälle huomiolle jäävä asia on tietojen hävittäminen asianmukaisesti.

7.1 Säilyttäminen

Paperisessa muodossa olevia asiakirjoja kertyy yleensä valtavasti, joten niiden säilyttäminen turvallisesti on yleensä aika hankalaa. Aivan salaisimmat ja tärkeimmät asiakirjat kannattaa kuitenkin säilöä esimerkiksi kassakaappiin, jossa ne ovat hyvässä suojassa. Myös lukolla varustettu kaappi tai pöytälaatikko on parempi kuin se, että asiakirjat ovat pinossa pöydän kulmalla. Tärkeä asia tietoaineiston säilyttämisessä on myös se, että kaikki tärkeät tiedostot ovat sijoitettu eri paikkoihin, jotta vahingon tai onnettomuuden sattuessa kaikki tiedot eivät tuhoudu samalla kertaa. Varmuuskopioita tulee säilyttää sellaisessa paikassa, jossa ne eivät voi tuhoutua alkuperäisen kopion mukana. Yritysten varmuuskopioiden säilytyksessä tulisi ottaa huomioon myös sellaisia riskejä kuin varkaus, tulipalo tai jopa luonnonmullistukset. Usein näitä asioita ei oteta tarpeeksi vakavasti, mutta sitten kun onnettomuus sattuu kohdalle, voivat tuhot olla mittavat. (Ruohonen, 2002, 210)

7.2 Hävittäminen

Yrityksille tulee jossakin vaiheessa eteen sellaisia asiakirjoja, joita ei tarvitse enää pitää tallessa. Esimerkiksi vanhat asiakas- tai projektitiedot joutuvat usein hävitettäväksi. Asiakirjojen hävittäminen oikealla tavalla on hyvin tärkeää. Paperisia asiakirjoja ei missään nimessä tule heittää ehjänä paperinkeräykseen tai roskiin. Joku ulkopuolinen voi mennä tutkimaan papereita ja saada käsiinsä jotain hyvinkin tärkeää ja salattua tietoa. Oman kokemukseni perusteella asiakirjojen hävittäminen onnistuu parhaiten ja helpoiten paperisilppurilla.

Erilaisten mediatallenteiden, kuten cd- ja dvd- levyjen hävittäminen jää monella usein tekemättä. Yleensä ne vain heitetään roskikseen. Vanhoilla levyillä voi olla kuitenkin hyvinkin arkaluontoisia asioita, joten nekin kannattaa hävittää asianmukaisesti. Nyky-

aikaisilla paperisilppureilla voidaan tuhota paperiasiakirjojen ohella myös cd- ja dvd-levyjä.

Yritysten tietokoneet menevät myös jossakin vaiheessa vanhaksi ja niistä täytyy päästä eroon. Vanhojen tietokoneiden kiintolevyt tulee myös hävittää tai tyhjentää perusteellisesti ennen hävitystä tai uudelleensijoitusta. Mikäli tietokone siirtyy johonkin muuhun käyttöön, täytyy kiintolevy tyhjentää perusteellisesti, ettei uusi käyttäjä pääse tietoihin käsiksi. Pelkkä kiintolevyn formatointi ei poista kaikkia tietoja levyltä, joten levy kannattaa viedä ammattilaisille tyhjennettäväksi. Jos tietokone mene kierrätykseen, kannattaa kiintolevy purkaa osiin ja naarmuttaa levyn sisäosat, jonka jälkeen kiintolevy on varmasti käyttökelvoton. (Symantec, 2007. 15,17)

8 TIETOTURVASUUNNITELMA YRITYKSELLE

Tietoturvasuunnitelma on laadittu sähkö- ja tietojärjestelmäsuunnittelua tarjoavalle yritykselle. Yrityksen nimeä ei työssä paljasteta tietoturvasyiden takia. Yritys työllistää tällä hetkellä 13 vakituista työntekijää. Yrityksen tietoteknisiä tarpeita on hoitanut tähän mennessä suunnittelupäällikkö sivutoimenaan. Yrityksellä on käytössään oma palvelin, jonka varmuuskopioiden ottamisesta hän on huolehtinut. Yritys on ostanut tarvittaessa tietotekniikka-apua eri yrityksiltä.

8.1 Hallinnollinen turvallisuus

Näin pienen yrityksen ei ole kannattavaa tehdä kovinkaan suuria muutoksia hallinnollisiin tietoturva asioihin. Tässä tilanteessa kannattaa tehdä korkeintaan pieniä lisäyksiä tietoturvapolitiikkaan. Yksi yrityksen työntekijöistä kannattaa palkata muun työn ohessa tietoturvavastaavaksi. Hänen tehtävänään on seurata yrityksen tietoturvan tasoa ja kehitystä. Tietoturvavastaavan täytyy varmistaa, että tietoturvavaatimukset otetaan huomioon esimerkiksi uusien laitteiden hankinnoissa ja tietojärjestelmän käytössä. Kaikkien yrityksen työntekijöiden täytyy tietenkin tehdä oma osansa tietoturvan toteutumisessa.

Tietoturvavastaavan tehtäviin kuuluu myös ajankohtaisista tietoturvaan liittyvistä asioista tiedottaminen ja kouluttaminen. Kaikille työntekijöille tulee antaa ohjeet, kuinka tietoturvaa toteutetaan. Perusperiaatteena voidaan sanoa, että työntekijän tulee ymmärtää tietoturvan merkitys omassa työssään sekä oppia tunnistamaan mahdolliset riskit. Tietoturvavastaavan kannattaa pitää kirjaa tietoturvaan liittyvistä tapahtumista, jonka perusteella saadaan selville millä tasolla yrityksen tietoturva on. Jokainen työntekijä on velvollinen seuraamaan tietoturvan tasoa ja kertomaan omat kehitysehdotukset tietoturvavastaavalle, joka tarvittaessa tekee muutoksia toimintaan.

8.2 Fyysinen turvallisuus

Kaikki tietoturvaan liittyvät asiat eivät liity pelkästään tietoteknisiin laitteisiin. Fyysiseen turvallisuuteen liittyvät toimitilat, joiden suojaukseen tulee kiinnittää paljon huomiota. Avaimilla on tässä asiassa tietysti todella suuri merkitys. Todella hyvin suojatusta rakennuksesta ei ole mitään hyötyä, jos joku ulkopuolinen on saanut käsiinsä yrityksen avaimen. Avaimesta huolehtimisen tärkeyttä ei voi korostaa koskaan liikaa.

Jokaiselle yrityksen työntekijälle on annettu oma avain ja jokaisen työntekijän omalla vastuulla on se, että siitä ei kukaan ota kopioita.

Yrityksen täytyy kiinnittää myös huomiota harvemmin tapahtuviin riskeihin, kuten tulipaloihin, vesivahinkoihin tai muihin vastaaviin vahinkoihin. Rahallisesti arvokkaimmat tietokonelaitteet ja asiakirjat tulee suojata siten, että ne eivät tuhoudu vesivahingon tai tulipalon sattuessa. Varashälytin on myös erittäin hyödyllinen. Tällä varmistetaan, että toimitiloihin murtautuessa varkaille ei jää niin paljon aikaa tehdä tuhoja tai viedä mukanaan arvokkaita laitteita, kun hälyttimet menevät päälle. Yrityksellä täytyy olla myös vakuutukset kunnossa erilaisten tapaturmien ja vahinkojen varalle. Vakuutukset eivät välttämättä korvaa kaikkia menetettyjä laitteita ja tietoja, mutta yritys voi kuitenkin saada rahallista korvausta. Yrityksessä on tällä hetkellä käytössä varashälyttimet, jotka työntekijät kytkevät päälle töistä lähtiessään. Mikäli viimeinen lähtijä unohtaa laittaa hälyttimet päälle, järjestelmä kytkeytyy kuitenkin automaattisesti päälle viimeistään kello 20.00.

8.2.1 Laitteistoturvallisuus

Kaikki yrityksen kaapeloinnit on suotavaa vetää siten, että ne kulkevat suojassa työpisteille, tulostimille ja palvelimelle. Tällä hetkellä yrityksen tietoliikennelaitteet ovat hyllyn päällä hieman huonossa suojassa. Tosin yrityksen toimitiloissa ei liiku valtavasti asiakkaita, joten laitteiden lähellä liikkuvat henkilöt ovat pääosin yrityksen työntekijöitä, jotka osaavat varoa paremmin laitteita. Tietoliikennelaitteet voivat mielestäni hyvinkin sijaita nykyisessä paikassa, mutta ne kannattaisi kiinnittää paikoilleen, etteivät ne pääse putoamaan hyllyltä, mikäli joku epähuomiossa nykäisee laitteiden kaapeleista.

Laitteita ei ole suojattu varkaudelta, mutta nämä laitteet eivät ole mahdollisten varkaiden ensimmäisiä kohteita, koska ne eivät sisällä mitään tietoa. Tosin yrityksen tärkein ja arvokkain tietotekninen laite eli palvelin sijaitsee samassa tilassa. Palvelin kannattaa suojata mahdollisimman hyvin, koska se sisältää paljon arvokasta tietoa. Olisikin vähintään suotavaa, että yritys siirtäisi palvelimen omaan lukittuun tilaansa, missä se ei ole näkyvillä ja se on hyvin suojattu tulipaloja, vesivahinkoja ja murtoja vastaan. Paras tapa suojata palvelin, on hankkia sille oma palvelinkaappi, missä se on hyvässä suojassa.

Normaalit pöytämalliset tietokoneet kannattaa sijoittaa pöydän alle asennettaviin telineisiin, mikäli se on mahdollista. Konetta ei kannata sijoittaa paljaalle lattialle, jossa

se on koko ajan potkittavana ja mahdollisen vesivahingon sattuessa se kastuu välittömästi. Tietokoneen johtojen asennukseen kannattaa myös kiinnittää huomiota. Johdot ja kaapelit olisi hyvä laittaa siististi nippuun ja kiinnittää vaikka pöytään ja seinään. Näin ne eivät ole muun muassa siivouksen tiellä.

8.2.2 Kulunvalvonta

Tällä hetkellä käytössä ei ole laitteistopohjaista kulunvalvontaa. Sihteerin toimisto on suoraan ulko-ovea vastapäätä, joten sihteeri pystyy ottamaan toimitiloihin sisään tulleet vastaan ilman, että kukaan pääsee liikkumaan tiloissa vapaasti. Toimitila on järjestelty siten, että asiakkaan tullessa paikalle työntekijät huomaavat helposti heidän tulonsa. Varsinainen laitteistopohjainen kulunvalvonta ei ole pakollinen, koska rakennus ei sijaitse ydinkeskustassa ja näin ollen toimitiloissa ei liiku koko ajan asiakkaita. Kulunvalvontaan pätevät samat asiat kuin muuhunkin tietoturvaan: Kaikkien työntekijöiden pitää tehdä oma osansa tietoturvan eteen. Jokainen huolehtii pois lähtiessään ovet lukkoon ja pitää huolen omasta avaimestaan.

8.2.3 Laitteiden kiinnittäminen ja merkintä

Kaikki vähänkin arvokkaammat tietotekniset laitteet tulee lukita fyysisesti pöytään kiinni varkauksien varalta. Muun muassa palvelin ja kalliit tulostimet kannattaa lukita. Nykyaikaisissa tietokoneissa (etenkin kannettavissa) on paikka vaijerilukolle. Näin mahdolliset varkaat eivät saa vietyä laitteita liian helposti. Kaikki laitteet tulee myös merkitä, jotta niistä on helpompi pitää kirjaa. Näin ollen viallinen kone on helpompi paikallistaa, kun sen kaikki tiedot on otettu ylös. Laitteista kannattaa ottaa ylös muun muassa sarjannumerot ja huoltohistoria, jotta niiden seuranta helpottuu.

8.2.4 Arkistot ja kassakaapit

Yrityksellä on paperimuodossa olevia asiakirjoja vielä paljon käytössä, joten niidenkin suojauksen täytyy olla kunnossa. Paperisten asiakirjojen suurimmat vaarat ovat tuli ja vesi. Nämä vaarat ilmaantuvat yleensä yhdessä paikalle. Asiakirjoille kannattaa hankkia laadukkaat lukoilla varustetut metalliset kaapit, joiden sisällä asiakirjoilla on suurempi mahdollisuus säästyä ehjänä, kuin esimerkiksi puisessa kaapissa. Metallinen kaappi on hyvä myös varkauksia vastaan. Asiakirjoja kannattaa säilyttää mahdollisimman paljon arkistossa. Tulipalon tai vesivahingon sattuessa pöydällä olevat asiakirjat tuhoutuvat todennäköisesti ensimmäisenä. Pöydällä olevat asiakirjat on myös helppo varastaa.

Pahimmassa tapauksessa yrityksen asiakas voi toimia toisen yrityksen vakoojana ja voi saada yrityksen pöydältä käsiinsä tärkeätäkin tietoa. Tällaisia tilanteita tapahtuu tietysti kohtuullisen harvoin, mutta se voi sattua kenen tahansa kohdalle ja siitä voi koitua erittäin suuret rahalliset tappiot. Työntekijöiden kannattaa pitää työpöydällään vain sillä hetkellä tarvitsemansa asiakirjat ja laittaa muut arkistoon. Näin toimiminen ei tule aina onnistumaan, mutta tähän kannattaa kuitenkin pyrkiä.

Yrityksellä on myös hyvä olla kassakaappi, jossa voidaan säilyttää kaikista arvokkaimmat asiakirjat ja muun muassa yrityksen mahdollinen kassa. Etenkin pienikokoisemmat kassakaapit kannattaa kiinnittää lattiaan, jotta niitä ei ole helppo varastaa. Yleensä kassakaapit ovat varkaiden ensimmäinen ja halutuin kohde. Yritys säilyttää tällä hetkellä muun muassa erilaisia varmuuskopioita kassakaapissa, mikä on erittäin järkevä idea, koska siellä ne pysyvät varmassa tallessa.

8.2.5 Siivous

Toimitilojen siivoaminen on pieni osa fyysistä turvallisuutta, mutta sitä ei suinkaan sovi unohtaa. Nykyaikaiset tietokonelaitteet ovat heikkoja sietämään pölyä. Pöly yleensä tukkii laitteiden tuuletuksen, mikä johtaa ylikuumenemiseen. Näin ollen laitteita ja niiden ympäristöä täytyy pystyä siivoamaan helposti. Varsinkin tehokkaammissa tietokoneissa on sisällä tuulettimet, jotka imevät viileää ilmaa sisälle. Jos ympäristö on pahasti pölyinen, kulkeutuu pöly myös helposti tietokoneen sisälle. Tietokoneet kannattaa pääsääntöisesti puhdistaa vähintään pari kertaa vuodessa, mieluummin useammin. Puhdistamisen voi hoitaa kaupasta saatavalla paineilmapullolla ja pölynimurilla. Tehokkaalla paineilmalaitteella puhdistamista ei suositella, koska suuri ilmanpaine voi irrottaa tietokoneen emolevyltä komponentteja. Johdot ja kaapelit täytyy kiinnittää siten, että ne eivät voi sotkeutua siivousvälineisiin.

8.2.6 Paloturvallisuus

Yrityksen tiloissa olisi hyvä olla jokaisessa huoneessa normaali palovaroitin, jotta tulipalon sattuessa hälytys menee päälle mahdollisimman nopeasti. Etenkin palvelimen lähellä on hyvä olla palovaroitin, koska se sisältää tärkeimmät ja arvokkaimmat tiedot. Palvelin sijaitsee monesti myös lukitussa huoneessa, joten mahdollisen tulipalon syttymistä ei välttämättä huomata riittävän ajoissa.

Yrityksen tiloissa täytyy olla selkeästi merkityt hätäuloskäynnit, jotta suuren tulipalon sattuessa kaikki henkilöt saadaan rakennuksesta nopeasti ulos. Yrityksen turvallisuutta voi helposti parantaa hankkimalla sammutuspeitto ja hiilidioksidi- tai jauhesammutin.

8.2.7 Sähkökatko

Yrityksen palvelinta ei ole suojattu tällä hetkellä virtapiikeiltä eikä sähkökatkoilta. Näin ollen olisi erittäin suotavaa, että yritys hankkisi palvelimelle UPS-laitteen. Se estäisi mahdolliset virtapiikit ja pitäisi palvelimen pystyssä sen aikaa, että se voidaan ajaa hallitus alas. Hyviä ja tunnettuja UPS-laitteiden valmistajia ovat Eaton ja APC.

Palvelimelle hankittava UPS- laite on hyvinkin suositeltavaa, mutta siitä ei ole mitään haittaa muillekaan tietokoneille. Mikäli tietokoneelle ei haluta hankkia UPS-laitetta, kannattaa vähintäänkin hankkia pistorasiaan ylijännitesuoja, joka estää virtapiikin kulkeutumisen tietokoneelle. Jos virtapiikki pääsee tietokoneelle asti, se voi pahimmassa tapauksessa polttaa kaikki tietokoneen komponentit. Kannettavat tietokoneet eivät tosin säikähdä pelkästä virtakatkosta, koska ne voivat toimia vielä jonkun aikaa omalla akullaan. Virtapiikki voi aiheuttaa tuhoja myös kannettavalle koneelle. Kannettavissa tietokoneissa olevat akut menettävät kapasiteettiään hyvinkin nopeasti, mikäli latausjohto pidetään koko ajan koneessa kiinni ja akku on paikallaan. Tästä syystä on suositeltavaa pitää akku irti kannettavasta ja käyttää pelkkää virtajohtoa. Tässä tapauksessa kone sammuu virtakatkon sattuessa, mutta käyttäjä voi itse valita omasta mielestään pienemmän pahan. UPS-laite auttaa kuitenkin tässä tilanteessa.

8.3 Henkilöturvallisuus

Yritys on henkilömäärältään hyvin pieni, joten kaikki työntekijät tuntevat toisensa ja näin ollen mitään suurempia muutoksia ei kannata lähteä tekemään, koska niistä ei ole mitään hyötyä. Jokainen työntekijä myös tietää oman työnsä kuvan ja kuinka salaisten tietojen kanssa toimitaan.

Nykyään erilaiset sosiaalisen median palvelut ovat erittäin suosittuja. Niitä kautta voi vaikka mainostaa omaa yritystä. Tunnetuimmat ja käytetyimmät sosiaalisen median palvelut ovat Facebook, Youtube ja Twitter. Yritys ei mainosta itseään sosiaalisen median välityksellä, mutta työntekijöillä voi olla käytössään käyttäjätilejä. Monet yritykset ovat kieltäneet näiden palveluiden käytön työkoneilla, mikä on sinällään järkevää, koska näiden palveluiden kautta on levinnyt monenlaisia haittaohjelmia. Pahim-

massa tapauksessa ulkopuolinen on saanut käyttäjien käyttäjätunnukset ja salasanat käyttöönsä. Erityisen tärkeää on muistaa se, että yrityksen sisäisessä verkossa ja sosiaalisissa palveluissa ei saa missään nimessä käyttää samoja käyttäjätunnuksia ja salasanoja. Mikäli yrityksen työntekijät käyttävät kyseisiä palveluita, on suotavaa, että selaimessa käytetään suojattua yhteyttä. Olisikin hyvin suositeltavaa, että yritys pohtii työntekijöiden kanssa, kuinka näiden palveluiden kanssa toimitaan.

8.4 Tietoaineistoturvallisuus

8.4.1 Säilyttäminen

Yrityksellä on käytössään palvelin, joka ottaa varmuuskopioita yrityksen tiedoista nauhavarmennusasemalle. Nauhoja säilytetään tällä hetkellä palvelimen päällä olevassa laatikossa ja osa nauhoista on kassakaapissa. Palvelimen päällä olevat nauhat täytyy siirtää myös kassakaappiin, koska varmuuskopioita ja alkuperäistä kopiota ei saa säilyttää samassa paikassa. Tärkeimmät asiakirjat ja varmuuskopiot kannattaa sijoittaa vähintäänkin kassakaappiin, jossa ne ovat suojassa mahdollisilta varkauksilta ja muilta vahingoilta, kuten tulipaloilta ja vesivahingoilta.

8.4.2 Hävittäminen

Vanhaksi tai turhaksi mennyt tietoaineisto täytyy hävittää asianmukaisella tavalla, koska ne voivat sisältää yritykselle hyvinkin tärkeitä tietoja, joista joku ulkopuolinen voi saada jonkinlaista hyötyä. Asiakirjoja ei tule koskaan heittää roskiin sellaisenaan. Paperimuodossa olevien asiakirjojen hävittäminen onnistuu parhaiten paperisilppurilla. Paperisilppurit silppuavat asiakirjat todella pieniksi paperinpalasiksi, joista on hyvin vaikea saada selvää, mitä ne sisältävät. Paperisilpun voi tämän jälkeen polttaa tai laittaa paperinkeräykseen. Uudemman malliset paperisilppurit voivat myös tuhota CD/DVD -levyt. Näin vanhaksi menneet tallennusmediat saadaan tuhottua myös varsin helposti.

Mikäli yrityksellä tulee erittäin paljon paperijätettä, on mahdollista hankkia yritykseen lukittava paperinkeräyslaatikko, josta papereiden hävitykseen erikoistunut yritys vie paperit hävitettäväksi.

8.5 Ohjelmistoturvallisuus

Yrityksen käyttäessä tai hankkiessa uusia ohjelmistoja täytyy olla varma, että ohjelmistojen lisenssit ovat kunnossa ja ohjelmat ovat laillisia kopioita. Mikäli käytössä

olevan ohjelman lisenssi ei ole kunnossa, voi siitä seurata todella suuret sakot. Ohjelmistojen hankinnat kannattaa näin ollen antaa täysin yrityksen tietoturvavastaavalle. Ohjelmistojen lisenssit ja asennusmediat kannattaa säilyttää varmassa tallessa, koska niitä tarvitaan usein myöhemminkin. Uusia ohjelmistoja hankittaessa kannattaa selvittää ohjelmiston jatkuvuus, käyttäjätuki ja ohjelman tietoturvaominaisuudet. Yleensä suurempien valmistajien ohjelmistoilla on pitkä jatkuvuus ja hyvä käyttäjätuki.

Uusien ohjelmistojen asennus kannattaa antaa tietoturvavastaavan tehtäväksi, että vältytään suuremmilta ongelmilta. Yrityksen kannattaa myös miettiä ohjelmistoja hankkiessa sitä, että sisältyykö siihen automaattiset päivitykset. Tietoturvan kannalta automaattiset päivitykset ovat hyvä asia. Tällöin tietoturvavastaava ei joudu aina asentamaan päivityksiä kaikkiin koneisiin käsin, vaan tietokone hoitaa päivityksen itse. Esimerkiksi Microsoftin Office -ohjelmisto ja F-Securen virustorjuntaohjelmisto päivittävät itsensä automaattisesti.

8.6 Palvelin

Yrityksellä on käytössä oma palvelin, jossa säilytetään projektien tietoja ja sen kautta toimii myös yrityksen oma sähköposti. Käyttöjärjestelmänä on Microsoftin Server 2003. Palvelin on merkiltään IBM Server X Series 236, joka sisältää RAID-ominaisuuden. Palvelin sisältää näin ollen itsensä varmuuskopioinnin, mikä on käytännössä pakollista. Palvelimesta otetaan myös varmuuskopioita nauha-asemalla. Palvelimella toimii myös Active Directory, joka sisältää käyttäjien sisäänkirjautumistiedot. Palvelimelle on asennettu myös F-Securen virustorjuntaohjelmisto.

Palvelin on tällä hetkellä sijoitettu yrityksessä yhden käytävän päähän pöydälle. Suojana on ainoastaan yksi puinen sermi, joka toimii vain näkösuojana. Tähän asiaan olisi hyvä saada mahdollisimman nopeasti muutos, koska nyt palvelin on näkyvillä ja näin ollen hyvin altis kaikenlaiselle vahingolle. Palvelin kannattaisi siirtää johonkin toiseen huoneeseen lukkojen taakse. Palvelimen suojaksi kannattaa myös hankkia palvelinkaappi, joka estää palvelinta kolhiintumasta ja suojaa mahdolliselta tulipalolta tai vesivahingolta. Palvelimessa ei myöskään ole minkäänlaista UPS-järjestelmää. Yritys ei kuulemma ole kärsinyt virtakatkoista, mutta mielestäni olisi silti järkevää hankkia pienempikin UPS, jolla pystytään takaamaan, että palvelimelta ei häviä tietoja virtakatkojen takia.

8.7 Varmuuskopiointi

Yrityksen palvelimeen on sijoitettu nauhavarmistusasema, joka on jo hieman vanhanaikainen, mutta kuitenkin yrityksen tiedonsiirtomäärään nähden riittävä. Yritys oli kokeillut lähiverkon kautta toimivaa varmuuskopiointijärjestelmää, mutta käytössä olevien ohjelmien yhteensopivuusongelmien takia siitä jouduttiin luopumaan. Nauhavarmistusasema ottaa palvelimen tiedosta varmuuskopiot jokaisen päivän päätteeksi, joka on hyvä aikaväli. Palvelimessa on käytössä myös RAID-järjestelmä, joka varmistaa lopullisesti sen, että palvelimen tiedot pysyvät tallessa.

8.8 Työasemat

Yrityksellä on käytössä pöytätietokoneita ja kannettavia tietokoneita. Tietokoneiden käyttöjärjestelmänä ovat Microsoftin tuotteet Windows XP ja Windows 7. Nämä ovat yleisesti käytettyjä käyttöjärjestelmiä, joten niissä on hyvin vähän yhteensopivuusongelmia ja Microsoftin käyttäjätuki on vielä tällä hetkellä myös XP:llä toiminnassa.

Tietokoneisiin on otettu käyttöön myös Windowsin automaattiset päivitykset, että käyttöjärjestelmä pysyy ajan tasalla. Virustorjunta- ja palomuuriohjelmistona on käytössä suomalainen F-Secure Client Security. Näin ollen tietokoneidenkin tietoturva on hyvällä mallilla. Näihin asioihin ei tarvitse sen kummemmin puuttua.

Kaikille työasemille on asetettu käyttöön myös käyttäjätunnukset ja salasanat, jotka on toteutettu Active Directory -palvelun kautta. Tämän palvelun avulla käyttäjät pääsevät käyttämään yrityksen palvelimella olevia tiedostoja. Mikäli käyttäjä haluaa päästä käsiksi palvelimen tietoihin, tulee sisään kirjautuminen tehdä tämän palvelun kautta. Mutta käyttäjät voivat käyttää tietokonetta myös järjestelmänvalvoja tunnuksilla, mikäli palvelimen tietoihin ei ole tarvetta päästä.

8.9 Laitteistoturvallisuus

8.9.1 Laitteiston hankinta ja hävittäminen

Yritykselle tulee eteen jossakin vaiheessa uusien tietokonelaitteiden hankinta. Laitteistoa hankittaessa tulee ottaa huomioon laitteiston tarjoamat tietoturvaominaisuudet. Tärkeä asia tietoturvan lisäksi ovat laitteiston jatkuvuuteen liittyvät asiat, kuten takuu, huolto ja varaosien saatavuus. Henkilökohtaisen kokemukseni perusteella helpoin tapa on hankkia tietokonelaitteet joltakin tunnetulta ja suurelta valmistajalta,

kuten Dell, Fujitsu tai HP. Näillä tunnetuilla ja suurilla yrityksillä takuuasiat ja huollot sujuvat helpommin. Näiden yritysten laitteisiin on yleensä saatavilla myös hyvin varaosia, mikäli niihin ilmenee tarvetta.

Kun uudet laitteet otetaan käyttöön, tulee niihin asentaa kaikki tarvittavat ohjelmat. Etenkin ajurit, virustorjunta, palomuuri ja käyttöjärjestelmän päivitykset tulee asentaa ennen kuin tietokone liitetään yrityksen verkkoon tai Internetiin. Ilman näitä päivityksiä ja ohjelmia tietokone on erittäin altis viruksille. Uudet laitteet kannattaa antaa ensimmäiseksi tietoturvavastaavalle, joka hoitaa päivitykset, ohjelmat ja asetukset kuntoon, ennen kuin tietokone otetaan virallisesti käyttöön.

Laitteiston poistamisen yhteydessä täytyy tietokoneiden muistit tyhjentää täydellisesti, jotta tietoihin ei sen jälkeen pääse käsiksi.

8.9.2 Kannettavat tietokoneet

Kannettavia tietokoneita käytettäessä suurin tietoturvariski on varkaus. Tämän takia kannettavat tietokoneet on suotavaa lukita toimistolla käytettäessä pöytään kiinni vaijerilukolla ja suojata kunnollisella salasanalla sekä tietokoneella olevat tärkeät tiedot kannattaa suojata jollakin kryptausohjelmalla.

8.9.3 Tallennusvälineet

Erilaisia kannettavia muistivälineitä käytettäessä täytyy niistä pitää erittäin tarkkaa huolta. Esimerkiksi USB-muistit ovat hyvin pienikokoisia ja sen takia ne voivat hävitä hyvin herkästi. Mikäli tärkeiden tietojen siirtämiseen käytetään muistitikkuja, kannattaa niiden sisältämät tiedot suojata salasanalla tai käyttää erillistä kryptausohjelmaa, joka pitää tiedot vain oikeiden käyttäjien saatavilla. Monien valmistajien USB-muistien mukana tulee kryptausohjelma, jolla tämän salauksen voi suorittaa. Suositeltavaa näiden muistien kanssa on se, että niissä ei kannata kuljettaa erittäin tärkeitä tiedostoja.

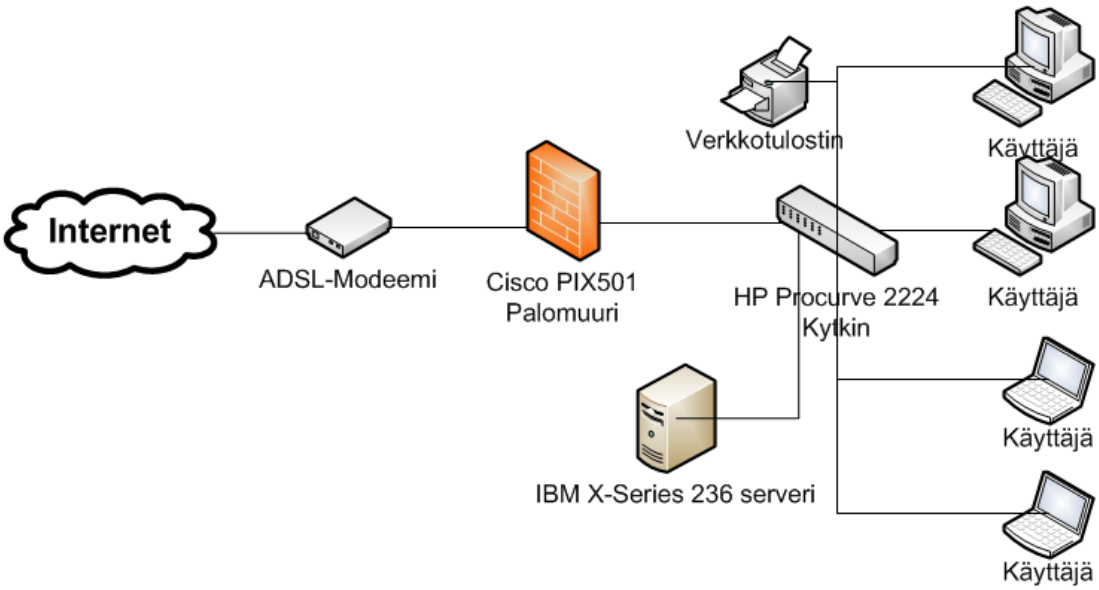
Kannettavien muistien käytöstä poistamisen kanssa täytyy toimia samalla tavalla, kuin tietokoneiden kiintolevyjenkin kanssa. Mikäli tikkuja käytetään vielä jossakin muussa käytössä, täytyy ne tyhjentää siten, että sinne ei jää mitään tietoa jäljelle. Ylimääräiset tikut kannattaa säilöä tulevaisuuden varalle lukittuun kaappiin. Mikäli muistia ei enää käytetä, tikku voidaan rikkoa fyysisesti, jolloin siitä tulee käyttökelvoton.

8.10 Tietoliikenneturvallisuus

Yritys on valinnut käyttöön Ciscon valmistaman palomuurin, joka pitää ylimääräiset tunkeilijat loitolla yrityksen kotiverkosta. Laitteessa on myös VPN ominaisuus, jonka avulla voidaan tehdä kannettavilla tietokoneilla etätyötä suojatusti.

Yrityksen palvelimella pyöritetään myös yrityksen omaa sähköpostia. Käytössä on Microsoftin Exchange Server -ohjelmisto, joka sisältää postipalvelimen, kalenterin ja roskapostisuodatuksen. Ohjelmisto on varsin kattava, joten siihen ei tarvitse hankkia erillistä roskapostinsuodatusta. Nykyään roskapostia on liikkeellä kuitenkin niin valtavasti, joten suodatin on käytännössä pakollinen.

Yrityksen tietoliikennelaitteet eivät enää ole ihan uusinta uutta, mutta niiden nopeus ja ominaisuudet ovat kuitenkin riittävät yrityksen tarpeisiin. Kuvassa kolme on yrityksen verkkokaavio, jossa näkyy myös laitteisto. Laitteet tukevat 10/100 megabitin LAN-verkon nopeuksia, jotka riittävät hyvin yritykselle. Kytkimenä on tällä hetkellä 24-porttinen HP:n Procurve, jonka ominaisuudet riittävät vielä tällä hetkellä. Suuren porttimäärän ansiosta verkon laajentaminen on myös mahdollista.



Kuva 3. Verkkokaavio yrityksen verkosta. (Miettinen, 2011)

8.11 Tietoturvasuunnitelman käyttöönotto

Yrityksessä oli työtä aloittaessani hyvä tietoturvan taso. Pienehköjä puutteita oli kuitenkin havaittavissa. Esimerkiksi työhuoneiden pöydillä oli varsin paljon erilaisia asiakirjoja, jotka olisi hyvä pitää vähintäänkin pöydän laatikoissa. Tämän suunnitelman tarkoituksena oli kuitenkin auttaa yritystä selvittämään tämänhetkinen tietoturvan taso ja mahdolliset puutteet. Näin ollen olisi hyvä, jos yritys perehtyisi tietoturvasuunnitelmaan ja pyrkisi korjaamaan esitetyt puutteet. Tässä työssä esitetyt parannusehdotukset eivät ole täydellisiä ja ainoita vaihtoehtoja, vaan yrityksen kannattaa pohtia erilaisia vaihtoehtoja. Osa tietoturvan asioista saattaa kuullosta pilkun viilaamiselta ja turhalta hössötykseltä, mutta se täytyy kuitenkin muistaa, että tietoturvan tason on vain niin hyvä, kuin sen heikoin lenkki. Kaikkien työntekijöiden täytyy jaksaa panostaa tietoturvaan.

8.11.1 Palvelin

Palvelin on tällä hetkellä sijoitettuna käytävän päähän pöydälle, jossa ei ole kuin näkösuoja edessä. Palvelin kannattaa sijoittaa vaikka johonkin työhuoneeseen, jossa liikkuu vähän työntekijöitä. Mikäli palvelinta ei voi sijoittaa toiseen huoneeseen kannattaa hankkia palvelinkaappi, jonka voi lukita. Palvelin pysyy kaapin sisällä suojassa ylimääräisiltä tunkeutujilta ja kolhuilta.

8.11.2 UPS

Yrityksellä ei ole tällä hetkellä käytössä ollenkaan UPS-laitteita, joten sellaisen hankkiminen on vähintäänkin suotavaa. Vaikka yrityksessä ei ole pitkään aikaan sattunut sähkökatkoksia, niin on kuitenkin kannattavaa hankkia laitteet mahdollisten katkojen varalle. Henkilökohtaisen mielipiteeni on se, että vähintäänkin palvelimella tulee olla UPS-laite.

8.11.3 Tietojen säilyttäminen

Palvelimessa olevan nauhavarmistusaseman nauhat olivat palvelimen päällä. Osa nauhoista oli kuitenkin viety kassakaappiin suojaan. Mutta jos tietoturvan taso halutaan pitää koko ajan korkeana, täytyy kaikki nauhat muistaa viedä kassakaappiin suojaan. Mikäli kassakaapin koko ei riitä kaikille varmuuskopioille, kannattaa vain uusimmat varmuuskopiot säilyttää kassakaapissa ja siirtää vanhempia varmuuskopioita hiljalleen muuhun lukittuun tilaan tai kaappiin.

Myös työhuoneiden pöydillä oli hyvin paljon asiakirjoja, joten se on myös tietoturvariski. Työpöydillä kannatta pitää vain työpäivän aikana tarvittavat asiakirjat ja työpäivän päätyttyä ne on hyvä laittaa vaikka lukittavaan työpöydän laatikkoon tai kaappiin.

8.11.4 Laitteiston puhdistaminen

Viimeisenä kohtana parannusehdotuksissa on vinkki, joka jää hyvin monelta huomioimatta. Tietoteknisiä laitteita ja niiden ympäristöjä kannattaa siivota erittäin usein, koska ne keräävät itseensä pölyä. Laitteiden käyttöikä paranee huomattavasti, kun niitä puhdistetaan säännöllisesti.

9 POHDINTA

Opinnäytetyön tavoitteena oli laatia toimiva ja etenkin hyödyllinen tietoturvasuunnitelma yritykselle. Suunnitelman tekeminen oli hyvin mielenkiintoista ja työtä tehdessä oppi koko ajan uusia tietoturvaan liittyviä asioita. Yrityksen tietoturva oli työtä tehdessä varsin hyvällä mallilla, joten mitään suuria muutosehdotuksia ei tarvinnut tehdä.

Työn tekemisen aikana ei tullut eteen mitään suurempia ongelmia. Pienenä yllätyksenä tuli kuitenkin se, että tietoturvasuunnitelmat eivät todellakaan liity pelkästään tietoteknisiin asioihin, vaan siinä otetaan huomioon hyvin paljon muutakin. Tietoturvasuunnitelmien yleinen laajuus vaikutti siihen, että työn rajauksen ja rakenteen kanssa meni aika paljon aikaa. Lähdekirjallisuutta tutkimalla sai kuitenkin hyvin paljon selvyyttä suunnitelmaan kuuluvista asioista.

Tavoitteeni työn kanssa oli se, että työstä olisi kohdeyritykselle aidosti hyötyä ja yritys tekisi ainakin osan ehdotetuista muutoksista tietoturvatoimintaansa. Toinen tavoite oli se, että tämän työn hyödyt eivät rajoittuisi pelkästään kohdeyritykseen, vaan suunnitelmaa olisi mahdollista käyttää pohjana muidenkin yritysten tietoturvasuunnitelmiin. Kehitettäviä tai lisättäviä asioita on muutama. Esimerkiksi yrityksen tietoturvaa olisi mahdollista tutkia myös erilaisilla teknisillä toimenpiteillä. Tässä työssä ei tekniseen tutkimiseen juurikaan perehdytty. Työn lopputulos on mielestäni onnistunut.

LÄHTEET

Diamantis, C. & Yamamura, Y. 2008. RAID (redundant array of independent disks) [viitattu 18.9.2011]. Saatavissa: http://searchstorage.techtarget.com/definition/RAID

Drake, J. 2007. Data Backup and Recovery Options. [viitattu: 18.9.2011].Saatavissa: http://www.infosecwriters.com/text_resources/pdf/Backup_JDrake.pdf

F-Secure. 2010a. Lehdistötiedote. [viitattu 17.9.2011] Saatavissa: http://www.f-secure.com/fi_FI/about-us/pressroom/news/2010/fs_news_20100215_02_fi.html

F-Secure. 2010b. Threat Types. [viitattu 17.6.2011]. Saatavissa: http://www.f-secure.com/en_EMEA-Labs/virus-encyclopedia/articles/classification/threat-types.html

Ferguson, P. & Huston, G. 1998. *What is a vpn?* [viitattu 18.9.2011]. Saatavissa: http://www.potaroo.net/papers/1998-3-vpn/vpn.pdf

Hakala, M.; Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Miettinen, J.E. 2002. Yritysturvallisuuden käsikirja. Helsinki: Talentum Media Oy

Pacific Gas and Electric Company. 2000 Uninterruptible Power supply [viitattu 21.9.2011]. Saatavissa: http://www.pge.com/includes/docs/pdfs/mybusiness/customerservice/energystatus/powerquality/ups.pdf

Patterson, D. ; Gibson, G. & Katz, R. 1988. A Case for Redundant Arrays of Inexpensive Disks (RAID) [viitattu 18.9.2011] Saatavissa: http://www-2.cs.cmu.edu/~garth/RAIDpaper/Patterson88.pdf

Rosendahl, M. 2011. Tietoturva kuuluu kaikille. [viitattu 18.9.2011]. Saatavissa: http://www.helsinki.fi/atk/lehdet/402/Tietoturva_kuuluu_kaikille.html

Ruohonen, M. 2002. Tietoturva. Jyväskylä: Docendo Finland Oy.

Symantec. 2007. Uskalla luottaa IT-ympäristöösi. Kristianstads Boktryckeri AB

Tietoturvan perusteet. 2005. Tietoturvan määritelmä. [viitattu: 18.9.2011]. Saatavissa: http://www.cibernarium.tamk.fi/tietoturva1/maaritelma_index.htm

Vance, A. 2010. If Your Password is 123456, Just Make It Hack Me. [viitattu 17.6.2011] Saatavissa: http://www.nytimes.com/2010/01/21/technology/21password.html

Wikimedia.2011 Palomuuri [viitattu 18.9.2011] Saatavissa: http://upload.wikimedia.org/wikipedia/fi/7/7d/Palomuuri_IT.png

ZAPware. 2011. VPN [viitattu: 18.9.2011] Saatavissa: http://www.zapware.ch/Sicherheit/vpn/