TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

OPINNÄYTETYÖRAPORTTI

PIENYRITYKSEN TIETOTURVA

Tapani Jarmas

Tietojenkäsittelyn koulutusohjelma
Joulukuu 2007
Työn ohjaaja: Harri Hakonen

TAMPERE 2007

TAMPEREEN
AMMATTIKORKEAKOULU

LIIKETALOUS

Tekijä(t): Tapani Jarmas

Koulutusohjelma(t): Tietojenkäsittely / Tietoverkkopalvelut

Opinnäytetyön nimi: Pienyrityksen tietoturva

Title in English: Security of a small enterprise

Työn valmistumis-kuukausi ja -vuosi: 12/2007

Työn ohjaaja: Harri Hakonen **Sivumäärä:** 54

TIIVISTELMÄ

Tietoturvaa käsitellään yleisessä keskustelussa useimmiten ainoastaan viruksentorjunnan ja palomuuriratkaisujen näkökulmasta, muiden tietoturvaan liittyvien asioiden jäädessä vähemmälle huomiolle. Tämän opinnäytetyön tarkoituksena on muodostaa kokonaiskuva tärkeimmistä pienyritysten tietoturvaan liittyvistä asioista ja ongelmista, sekä antaa pienyrityksille käytännön vinkkejä tietoturvan toteuttamiseen.

Työn teoriaosuudessa käydään läpi tietoturvan toteuttamisen perusteita (mm. tietoturvauhat ja laitteistot), sekä yritystoiminnassa huomioon otettavia asioita (henkilöstön kouluttaminen ja yrityskohtaiset tarpeet). Lopuksi luodaan teoriaosuudessa esiteltyjen asioiden pohjalta käytännön esimerkkiratkaisu tietoturvan teknisestä toteuttamisesta pieneen yritykseen.

Työssä painotetaan tietoturvaratkaisujen merkitystä yrityksen turvallisuuden kannalta. Se toimii johdatuksena laajaan aihepiiriin ja yrityksen henkilöstön tietoturvatietämyksen lisäämiseen.

Avainsanat: Tietoturva Tietojärjestelmät Tietoverkot Työntekijät Uhka

TAMPERE
POLYTECHNIC

BUSINESS SCHOOL

Author(s): Tapani Jarmas

Degree Programme(s): Business Information Systems

Title: Security of a small enterprise

Month and year: December/2007

Supervisor: Harri Hakonen **Pages:** 54

ABSTRACT

Information security is normally discussed from the view of firewall´s and antivirus software. Other relevant information is left a side. The purpose of the whole process is to establish some kind of picture, about the most important and relevant matters of information security. I also give some practical examples, how to carry out information security

In the theoretical part I will go through the basics of information security (among other things, information threats and hardware) and matters which have to have attention in entrepreneurship (education of employees and needs of the enterprise). In the end I will put into practice the theoretical part through an example of technical implementation of information security in a small enterprise.

The study highlights the information solutions considering the enterprises information safety. The work acts as a introduction to bigger subject on the matter and as a mentor to the employees.

Keywords: Information security Information system Network Employee Threat

1 Johdanto

Tietojenkäsittelyä opiskellessani olen huomannut, että mediassa puhutaan paljon palomuureista ja virustorjunnasta käsiteltäessä tietoturvaa. Harvemmin käsitellään muita tietoturvaa koskevia asioita, jotka ovat kuitenkin mielestäni yhtä tärkeitä. Tästä sain idean tutkintotyöni aiheeksi. Pohtiessani aiheen rajausta ja näkökulmaa ajattelin, että sopiva kohderyhmä voisivat olla pienet yritykset. Isäni on yrittäjä ja tuttavapiiristäni löytyy monia yrittäjiä, joiden toimintaa seuratessani olen havainnut, kuinka paljon puutteita on yrittäjien tietotuvassa. Tämän tutkintotyön tarkoitus on käytännön esimerkein esittää, kuinka tietoturva tulisi toteuttaa pienessä yrityksessä. Yritän kirjoittaa asioista mahdollisimman yksinkertaisesti, koska kohderyhmänä ovat kuitenkin pienyrittäjät eivätkä IT-alan ammattilaiset.

Tässä tutkintotyössä joudun tyytymään vain raapaisemaan pintaa tietoturvaan liittyvistä tärkeistä asioista, sillä lähes jokaisesta käsitellystä osa-alueesta voisi tehdä oman tutkimuksensa. Tavoitteena on siis tehdä tiivistetty esitys tietojärjestelmien ja -verkkojen varmistamisesta ja suojaamisesta, käymällä läpi tärkeimmät niihin liittyvät aihealueet.

En käsittele kovin laajasti virustorjuntaa tai palomuureja, koska niistä löytyy erittäin paljon materiaalia muutenkin. Keskityn lähinnä verkon rakenteeseen, laitteisiin, käyttöjärjestelmän asetuksiin ja tietoturvakäytäntöihin. Käyn myös läpi yleisiä tietoturva-asioita, jotka liittyvät laitteiden sijoitteluun sekä yrityksessä liikkumiseen (kulunvalvonta). Käyn lyhyesti läpi perustietoturvan rakenteen mukaan lukien virustorjuntaohjelmistot, sekä rauta- ja ohjelmistopalomuurit.

Pyrin selvittämään, mitä asioita yrityksen tulee huomioida tietojärjestelmissä ja kuinka minimoidaan ihmisten aiheuttamat ongelmat. Tarkastelen myös yleistyvien langattomien verkkojen tietoturvan toteuttamista sekä tietojen säilymisen turvaamista varmuuskopioinnilla.

Laitteista käyn läpi verkon toteuttamiseen tarvittavat laitteet ja selvitän, kuinka niiden asetuksilla sekä käytöllä voidaan parantaa tietoturvaa. Esittelen myös muutamia laitteita, jotka ovat hyödyllisiä erilaisissa tilanteissa. Tällaisia tilanteita voisi olla esimerkiksi ukonilma tai sähkökatkos.

2 Tietoturvan toteuttaminen

Tietoturvalla käsitetään kaikki mahdollinen tiedonturvaaminen, oli se sitten paperilla, sähköisessä muodossa, kuvina, ihmisten päässä jne. Meillä kaikilla on tietoja, joita haluamme pitää turvassa, pankkitunnuksista vanhoihin valokuviin. On siis erittäin olennaista, että perehdymme tapoihin ja menetelmiin, joilla voimme säilyttää mahdollisimman tehokkaasti näitä tietoja.

On tärkeää tietää, miten toteuttaa yrityksen sisäinen verkko tietoturvallisesti. Tietoturvaan kuuluu tietenkin kaikki muukin yrityksen toiminta. Kaikki tieto olisi syytä turvata ulkopuolisilta ja sisäpuolisilta uhilta.

2.1 Yleistä

Tietoturva käsittää paljon muutakin kuin virustorjunnan ja palomuurit. Usein puhutaan vain näistä kahdesta käsitteestä ja mainitsematta jää monia muita olennaisia seikkoja. Tietokoneet ovat alttiita laitevioille, kuten muukin elektroniikka. Kannattaa myös muistaa, että erilaiset onnettomuudet ja vahingot voivat aiheuttaa vahinkoa. On siis syytä varmistaa tietojen säilyminen esimerkiksi tulipalon sattuessa.

Tietoturvan tavoite on varmistaa, että tietokoneet ja niissä olevat ohjelmat tekevät aina sen, mitä niiden on tarkoitus tehdä eikä mitään muuta. Toisin sanoen suojata tietojärjestelmät mahdollisimman monelta odotetulta ja odottamalta riskiltä. Varmistaa, että järjestelmän suojattavat tiedot ovat niiden käyttöön oikeutettujen käyttäjien käytettävissä ja että nämä tiedot ovat näiden käyttäjien käytettävissä aina, kun he niitä tarvitsevat. Tietoturvan tavoitteet on jaettu näihin tietoturvapalveluihin: luottamuksellisuus, autenttisuus (oikeellisuus), kiistämättömyys, eheys ja käytettävyys. (Ruohonen 2002, 2.)

Viime vuosina tietoturva on huomattavasti monimutkaistunut, ja siihen liittyvät ongelmat eivät kosketa enää ainoastaan suuria yrityksiä vaan myös pienyrityksiä sekä kotikäyttäjiä. Enää ei riitä, että tärkeät tiedot ovat lukitun oven takana ja tietokoneissa on virustorjuntaohjelmat sekä palomuurit kunnossa. Suurin uhka yrityksen tietojärjestelmään kohdistuu nykyään sisäpuolelta eli työntekijöistä ja järjestelmän rakenteesta. Yritykset eivät yleensä ole ajatelleet, että tietoturvauhka voisi olla yrityksen sisällä. Mediassa on usein puhuttu palomuurien ja virustorjunnan tärkeydestä, ja moni yritys tuudittautuu ajatukseen, että heillä edellä mainitut asiat ovat kunnossa, vaikka todellisuus olisi toinen.

Yritysten työntekijöille hankitaan kannettavia tietokoneita ja muistitikkuja, joilla he voivat tehdä töitä muualla ja siirrellä materiaalia. On muistettava, että uhka on joka puolella ja voi iskeä silloin, kun sitä vähiten odottaa. Voimme esimerkiksi olla hieman huolimattomampia käyttäessämme laitteita työpaikan ulkopuolisessa ympäristössä.

Työntekijöistä on tullut suurin tietoturvauhka yrityksille. Heitä ei ole koulutettu tarpeeksi hyvin tiedostamaan ja havaitsemaan mahdollisia uhkan aiheuttajia. Tietokoneen käyttäjä voi altistaa yrityksen tietojärjestelmän monille uhille vahingossa tai tarkoituksella. Sen takia on erityisen tärkeätä kiinnittää huomiota työntekijöiden osaamiseen sekä oikeuksiin tietojärjestelmässä.

Tietoturva ei pelkästään käsitä viruksia, matoja, troijalaisia ja ulkopuolisia tietomurtoyrityksiä (hakkerit), vaan myös tavanomaisia ohjelmisto- sekä laitehäiriöitä/vikoja, tulipaloja, vesivahinkoja, ukonilmoja, henkilön huolimattomuutta ja vastaavanlaisia asioita. Uhkia on monenlaisia ja niitä vastaan kannattaa suojautua. Voimme kuvitella, kuinka monella yksityisyrittäjällä on kaikki yrityksen olennainen tieto yhdellä tietokoneella ja viimeiset varmuuskopiot otettu puoli vuotta sitten, jos niitä ylipäätään on otettu. Kovalevyn hajotessa katoaa suurin osa yrityksen tiedoista. Tällaiseen tilanteeseen tuskin yksikään yritys haluaa. Vastaava tilanne saisi jo monen kotikäyttäjänkin varuilleen.

Vahinkoa yritetään tehdä tunkeutumalla yritysten tietojärjestelmiin, tuhoamalla tietoja ja muuntelemalla kohteen nettisivuja. Roskaposteilla yritetään tukkia tiedonkulkua ja levittää viruksia. Hyökkäyksien ylikuormitus voi pahimmassa tapauksessa kaataa koko järjestelmän tai sulkea Internet-sivuston. Olemme myös saaneet lukea mediasta kuinka rikolliset yrittävät varastaa identiteettejä, luottokorttitietoja sekä pankkitunnuksia. (Myhr ym. 2004, 7.)

Tietojärjestelmän tietoturva jaetaan yleensä näihin osa-alueisiin:

- tietoaineiston turvallisuus
- ohjelmisto turvallisuus
- tietoliikenneturvallisuus
- fyysinen turvallisuus
- laitteistoturvallisuus
- henkilöstöturvallisuus
- käyttöturvallisuus
- hallinnollinen turvallisuus.

(Ruohonen 2002, 4.)

2.2 Palomuurit

Palomuurilla (firewall) pyritään estämään ei-haluttujen pakettien pääsy julkisesta verkosta (esimerkiksi Internetistä) suojattuun verkkoon (esimerkiksi yrityksen lähiverkkoon tai kotikoneelle) suodattamalla ne tietoliikenteestä. Palomuurina voi toimia erillinen laite, reititin tai tietokoneessa oleva ohjelma (jonka kautta suodatettava tietoliikenne kulkee). (Ruohonen 2002, 64.)

Palomuuri on tietoturvajärjestelmä, joka suojaa yleensä sisäverkkoa/tietokonetta ulkopuolisilta hyökkäyksiltä ja murtautumisyrityksiltä. Muurilla pystytään lisäksi piilottamaan sisäisen verkon rakenne. Palomuuri tutkii liityntäänsä saapuvan liikenteen ja soveltaa siihen tiettyjä sääntöjä, käytännössä sallien tai estäen liikenteen kyseisten sääntöjen perusteella. Palomuuri suodattaa sekä saapuvan että lähtevän liikenteen. (Thomas 2004, 161.) Sen tehtävä on siis tarkkailla liikennevirtaa ja havaita mahdolliset osoiteväärennökset, sekä kaato- ja häiriöyritykset. Palomuurit voidaan jakaa toteutustapansa perusteella kolmeen ryhmään: pakettisuodattimet, Proxy-palomuurit ja tilatietoiset palomuurit.

Isommissa yrityksissä käytetään useampia palomuureja, koska niillä on yleensä laajat tietoverkot ja ne tarjoavat erilaisia verkkopalveluja asiakkailleen, esimerkiksi nettikaupan, ekstranetin ja intranetin. Yleensä nämä sijoitetaan omille julkisille palvelimille. Tällaista aluetta usein kutsutaan eteisverkoksi eli demilitarisoitu alue (DMZ, demilitarized zone). Tällaisessa tapauksessa siis ensimmäinen palomuuri sijaitsee luotetunverkon (DMZ) ja Internetin välissä. Eteisverkon ja sisäverkon välissä sijaitsee toinen palomuuri.

Palomuuri ei kuitenkaan nykyään riitä aina suojaamaan yrityksen verkkoa. On muitakin tapoja ohittaa palomuuri kuin hakkeroimalla sen läpi. Kaikki, jotka pääsevät verkkoon käsiksi yrityksen sisältä ovat sinällään uhka, kuten yrityksen henkilökunta ja vieraat, jotka tuovat mukanaan kannettavia tietokoneita, jotka liitetään yrityksen sisäverkkoon. WLAN-tukiasemat (Wireless Local Area Network) saattavat päästää liikennettä sekä ulos että sisään palomuurin ohi. Näissä tapauksissa tietokoneissa mahdollisesti olevat haittaohjelmat pääsevät leviämään lähiverkkoon.

2.3 Virustorjunta

Virustorjuntaohjelmien on tarkoitus havaita ja paljastaa tiedostoissa mahdollisesti olevat virukset, madot ja Troijan hevoset. Virussuojaus tulisi olla kaikissa Internet-yhteyttä käyttävissä palvelimissa ja työasemissa. Nykyään virustorjuntaohjelmien on pystyt-

tävä kehittymään ja pysymään muuttuvien uhkakuvien mukana. Tämän takia on erittäin tärkeätä, että kaikissa laitteissa on ajan tasalla oleva ohjelmisto. Ohjelmistojen tarjoajat tekevät ohjelmiin nykyään virusmääritelmiä, jotka pystyvät vertaamaan epäiltyä uhkaa lähetettyyn määritelmään. Ohjelman toimittajat lähettävät eräänlaisen digitaalisen sormenjäljen aina, kun uusi uhka paljastuu.

Virustorjuntaohjelmat etsivät ja tuhoavat järjestelmästä haitallisia prosesseja, niiden tarvitsemia tiedostoja ja muiden ohjelmien tiedostoihin tarttuneita haitallisia koodeja. Tietyt virukset yrittävät lamauttaa tietokoneelta virustorjunnan prosesseja tai häiritä niiden toimintaa. Virustorjuntaohjelmien toimintaan kuuluu suojata tietokoneella tai palvelimella olevia tiedostoja, joihin virukset usein yrittävät tunkeutua tekemään muutoksia ja/tai lukemaan laitteen tietoja pystyäkseen toimimaan vapaammin, sekä estääkseen virustorjunnan toiminnan tai levitäkseen seuraavaan koneeseen.

Nykyään ei enää leviä kovin paljon perinteisiä viruksia. Virusten tekijät ovat alkaneet tuottamaan matoja. Viruksia muistuttava mato levittää itseään haitallisen koodin tarkkoina kopioina, jotka siirretään toisiin tietokoneisiin ja käynnistyvät automaattisesti. (Myhr ym. 2004, 22.) Matojakin on monenlaisia, niin verkossa kuin sähköpostitse leviäviä. Viruksia on myös nykyään alkanut esiintyä muissakin laitteissa, kuten puhelimissa ja auton elektronisissa järjestelmissä. Tämä on tullut mahdolliseksi Bluethoot-yhteyksien ja puhelimien monipuolisten toimintojen kautta (verkkoselaimet).

2.3.1 Muita haittaohjelmia

Haittaohjelmia on muitakin kuin virukset, madot ja Troijan hevoset. Se on yleiskäsite kaikille ohjelmille, jotka aiheuttavat tarkoituksella vahinkoa sekä ei-toivottuja tapahtumia tietokoneilla ja tietojärjestelmissä. Tällaisia haittaohjelmia ovat vakoiluohjelmat (spyware), rootkitit, mainosohjelmat (adware), takaovet (backdoor). Tämän kaltaisille ohjelmille on olemassa siivousohjelmia, jotka havaitsevat ja poistavat ne. Monissa tietoturvapaketeissa tulee mukana ominaisuuksia, joilla nämä ohjelmat saadaan poistettua.

Vakoiluohjelmat vakoilevat ja keräävät tietoja käyttäjän toimista, kuten käytyjen Internet-sivustojen osoitteita, salasanoja tai luottokorttitietoja ja lähettävät ne isännälleen.

Rootkit on ohjelmisto, jonka hyökkääjä voi asentaa koneelle saatuaan sen hallintaansa. Ohjelma pyrkii piilottamaan itsensä tuhoamalla mahdollisia jälkiä tartunnasta ja piilottamalla mahdolliset prosessinsa sekä verkkoyhteydet. Rootkiteissä on usein myös etähallintaominaisuus.

Mainosohjelma on usein helppo havaita, ja nimikin kertoo niiden toiminnan. Kyseinen ohjelma avaa mainoksia tietokoneen ruudulle, ja yleensä ne aktivoituvat, kun Internet-selain avataan. Nämä ohjelmat asentuvat muiden, yleensä ilmaisohjelmien mukana, joita voi netistä ladata tai tietoturva-aukkojen kautta. Mainosohjelmat yrittävät myös ottaa yhteyttä isäntäkoneeseensa.

Takaovi on ohjelma, jonka tarkoituksena on sallia vieraalle pääsy tietokoneeseen normaalit tietoturvamekanismit ohittaen. Takaovi-ohjelma yritetään asentaa tietokoneelle käyttäjän huomaamatta, usein tietoturva-aukkojen kautta se voi tulla viruksen tai madon mukana. Ohjelma voi olla myös sisäänrakennettuna toisessa ohjelmassa.

2.3.2 Anti-spyware ohjelmat

Vakoiluohjelmien torjuntaan on myös kehitetty ohjelmia. Näillä ohjelmilla on lähinnä kaksi keinoa puolustautua haitallisia ohjelmia vastaan: ajantasainen suojaus, joka estää vakoiluohjelmien asennuksen, sekä niiden paikannus ja poistaminen. Torjuntaohjelmat tutkivat Windowsin rekisterin, asennetut ohjelmat ja käytössä olevat järjestelmätiedostot. Tämän jälkeen torjuntaohjelmat poistavat tiedostoista ne, jotka ohjelma havaitsee vakoiluohjelmien listaltaan. Vakoiluohjelmasuojaus toimii siis samalla tavalla kuin vastaavat virussuojausohjelmat. Samalla lailla kuin virustorjuntaohjelmia, niin myös anti-spyware -ohjelmia on päivitettävä, että ne toimivat tehokkaasti.

Internetistä löytyy monia ilmaisohjelmia, jotka ovat erittäin hyödyllisiä ja toimivia haittaohjelmien poistamiseen. Mainitakseni muutamia: Ad-Aware, Spyware doctor, Spybot, CWShredder, jne. Itse olen hankkinut ohjelman nimeltä Hitman Pro, joka on eräänlainen skriptiohjelma, joka ajaa useita ilmaisia haittaohjelmien poistajia ja poistaa haittaohjelmat, sekä lopuksi antaa raportin toimenpiteistä.

Nykyään monet virustorjuntayhtiöt ovat lisänneet virustorjuntaohjelmiinsa anti-spyware -ominaisuudet osaksi suojausta. Näin ovat toimineet ainakin Symantec ja F-Secure. Kannattaa myös muistaa, että selaimiin saa nykyään lisäohjelmia, joilla pystytään estämään erilaisia ohjelmia käynnistymästä nettisivuille mentäessä. Lisäksi löytyy lisäohjelmia joille voi opettaa huonoja ja haitallisia sivustoja.

2.4 IDS (Intrusion Detection System)

Uusimpia tietoturvan parantamismenetelmiä tai -ohjelmia ovat tunkeutumisen havaitsemisjärjestelmät (Intrusion Detection System eli IDS). IDS:n toiminta perustuu kolmeen edellytykseen: missä vahditaan, mitä vahditaan ja miten vahditaan. (Thomas 2004, 322.)

Ensimmäinen edellytys, missä vahditaan, kertoo mihin IDS loogisesti sijoitetaan tarkkailemaan tapahtumia. Toinen edellytys, mitä vahditaan, kertoo IDS:lle millaisissa tilanteissa sen tulee tehdä hälytys tai ryhtyä joihinkin muihin toimenpiteisiin. Kolmas edellytys, miten toimitaan, määrää miten IDS toimii, kun tilanne täyttää tietyt odotusarvot. IDS toimii todellisuudessa siis seuraavasti:

1. IDS asennetaan vahtimaan Internet-liityntää ja niitä, jotka yrittävät päästä verkkoon palomuurin läpi.
2. IDS:lle kerrotaan, minkä tyyppisiä hakkerointitoimenpiteitä ja hyökkäyksiä sen tulee etsiä paketti- ja yhteystyypin perusteella ja mitä vastatoimenpiteitä mahdollisesti tulee suorittaa.
3. IDS:ää kehotetaan lähettämään hyökkäyksen tapahtuessa viesti verkkovastaavan matkapuhelimeen ja sähköpostiin.
4. Hakkeri pyrkii verkkoon porttiskannauksella, joka skannaa ensimmäiset tuhat TCP-porttia (Transmission Control Protocol).
5. IDS näkee näihin portteihin kohdistuvat peräkkäiset yhteysyritykset, tarkistaa tietokantansa ja havaitsee että tällainen käyttäytyminen vastaa sinne syötettyä porttiskannausprofiilia.
6. IDS yrittää lähettää samanaikaisesti viestin verkkovastaavan sähköpostiin ja matkapuhelimeen.
7. Yhtäkkiä porttiskannauksen määrä kasvaa ja skannauksia tulee myös toisesta lähteestä.
8. IDS ilmoittaa tästäkin yrityksestä.

(Thomas 2004, 323.)

IDS ei kuitenkaan ole täydellinen järjestelmä, siinäkin on puutteita. Se pitää konfiguroida oikein, että IDS toimii järkevästi. IDS ei pysty kuin valvomaan yhtä liitäntää kerrallaan. Lopuksi IDS:stä voi tulla hakkerin liittolainen. Jos verkkovastaavan matkapuhelin alkaa täyttyä IDS:n lähettämistä viesteistä, hän alkaa suodattaa niitä vääränä hälytyksinä. Tällöin hän saattaa jättää huomioimatta viestejä, joilla on merkitystä. IDS-järjestelmät eivät ole täydellisiä ja nekin antavat aika ajoin vääriä hälytyksiä. Hakkerit myös opettelevat eri turvautumistapojen toimintaa ja kuinka niitä voidaan huijata tai hyödyntää. (Thomas 2004, 323.)

IDS:ä on kahden tyyppisiä, eli isäntäpohjaisia tunkeutumisen havaitsemisjärjestelmiä (HIDS, Host Intrusion Detection System) ja verkkopohjaisia tunkeutumisen havainnointijärjestelmiä (NIDS, Network Intrusion Detection System) (Thomas 2004, 330).

NIDS kaappaa kaikki paketit siinä segmentissä, johon se on liitetty. NIDS muistuttaa pakettien nuuskimista, mutta toimii paketin siepattuaan eri tavalla. Se toimii salakuuntelumallin mukaisesti ja voidaan toteuttaa parilla eri tavalla:

- Kaapelin salakuuntelu – Menetelmässä paketit kaapataan kahden verkkolaitteen välille sijoitetun fyysisen haaraliitoksen kautta, johon NIDS liitetään.
- Portin peilaus – Kytkimestä riippuen voi joustavampi ratkaisu olla portin peilaus eli portin skannaus. Tässä tekniikassa kytkin ohjataan lähettämään peilaavaan porttiin kopio jokaisesta paketista, joka on menossa esimerkiksi palomuurin sisältävään porttiin. NIDS on liitetty peilaavaan porttiin.

(Thomas 2004, 330.)

Kun NIDS lukee paketteja, ne voidaan analysoida eri tavoin riippuen siitä, millainen NIDS on kyseessä. Jotkin NIDS-järjestelmät etsivät sormenjälkeä vertaamalla pakettia tietokannassaan oleviin hyökkäystunnusmerkkeihin. Toiset etsivät epätavallista pakettiliikennettä, joka voisi kertoa käynnissä olevasta hyökkäyksestä. (Thomas 2004, 330.)

HIDS:t tarkkailevat tietyn palvelimen järjestelmätoimintoja, sekä palvelimeen kohdistuvia hyökkäyksiä ja reagoivat hyökkäyksiin. Toisin kuin NIDS, HIDS asennetaan tarkkailtavaan isäntään, esimerkiksi web- tai postipalvelimeen. HIDS tarkkailee isännän tarkastus- ja tapahtumalokeja, kun NIDS puolestaan tarkkailee paketteja. HIDS ei pyri vertailemaan pakettien sisältöä hyökkäystunnusmerkkeihin, vaan tunnistamaan tunnettuja malleja, jos paikalliset tai etäkäyttäjät tekevät kiellettyjä asioita. (Thomas 2004, 331.)

HIDS toimii kuin virustorjuntaohjelmisto (vaikka ei korvaa sitä), ja sen laajennetut ominaisuudet voivat parantaa suuresti verkon tietoturvaa. HIDS sopii parhaiten isäntiin kohdistuvien tietoturvauhkien vastaiseen taisteluun, koska se pystyy tarkkailemaan palvelimen käyttäjien toimenpiteitä, sekä tiedostohakuja ja reagoimaan niihin. Suurin osa tietokoneisiin kohdistuvista uhista tulee organisaation sisältä monista eri lähteistä, kuten tyytymättömiltä työntekijöiltä tai yritysvakoojilta. HIDS tarkkailee palvelimia ja tarjoaa tietoa seuraavista seikoista:

- Tunkeutumisyritykset, onnistuneet tunkeutumiset ja valtuutettujen käyttäjien epäilyttävä käyttäytyminen.
- Isännän skannauksella varmistetaan, että hyväksyttyjä tietoturvakäytäntöjä noudatetaan, kuten viimeisempien päivitysten tekeminen ja turhien palvelujen poiskytkentä.
- Tarkastuskäytännön hallinta ja keskittäminen, todistusaineiston kerääminen, tilastoanalyysi ja tiedot tapahtumista, eräissä tapauksissa myös pääsynvalvonta. Toiminnot ovat yleensä tuettuina järeämmissä työkaluissa.

(Thomas 2004, 332.)

IDS pystyy kokoamaan pakettivuon uudelleen istunnoksi ja analysoimaan, mitä todellisuudessa tapahtuu. Prosessi on erittäin tärkeä, koska sen avulla IDS voi koota tapahtumia yhteen ja tarjota hallintatyöasemalle tarvittavan tapahtumien korreloinnin. Korrelointi on yhä tärkeämpää. Näin voidaan esimerkiksi havaita työntekijöiden kannettavilla koneilla mahdollisesti olevat verkkomadot ja vastaavat ohjelmat. Kannettaviin olisikin hyvä asentaa HIDS. (Thomas 2004, 333.)

2.5 Houkutuslinnut

Houkutuslintu on joustava, Internetiin yhdistetty tietokonejärjestelmä. Se on räätälälöity tietoturvatyökaluksi ja asennettu varta vasten houkuttelemaan ansaan henkilöitä, jotka yrittävät päästä toisten tietokonejärjestelmiin tunnustelemalla, skannaamalla ja tunkeutumalla. Kohderyhmään kuuluvat hakkerit, krakkerit ja script kiddiet (ks. s.15) riippumatta siitä, mistä päin maailmaa he ovat. (Thomas 2004, 345.)

Houkutuslinnut eivät ratkaise yhtään tietoturvaongelmaa. Sen sijaan niitä käytetään harhautuksiin, torjuntaan, havaitsemiseen ja tietojen keräämiseen. Ne on suunniteltu tarkoituksella muistuttamaan jotakin sellaista (esim. POP3-postipalvelin), mihin hyökkääjät pyrkivät hakkeroimaan, ja niitä tarkkaillaan tiiviisti. Houkutuslintua ei tule käyttää tuotannossa, sillä houkutuslintua tunnustellaan, siihen hyökätään, tai siihen pyritään murtautumaan. Houkutuslinnut palvelevat seuraavia tärkeitä tarkoituksia:

- Houkutuslinnut harhauttavat hyökkääjiä pois tärkeimpien verkkoresurssien kimpusta, jolloin verkon suojaaminen on helpompaa.
- Houkutuslintujen avulla voidaan saada ennakkovaroitus uusista hyökkäyksistä ja tunkeutumisyrityksistä. IDS voi tuottaa vääriä hälytyksiä. Vahingoittamispyrkimykset puolestaan kohdistuvat ainoastaan houkutuslintuun, joka ei ole tuotannossa.

- Houkutuslintujen ansiosta hyökkääjän toimintaa voidaan tutkia tarkasti, sekä houkutuslintuun kohdistuneen hyökkäyksen aikana että sen jälkeen. Voi tuntua siltä, että tämä kiinnostaa vain tutkijoita, mutta tällä tavalla on myös mahdollista oppia asioita, joista on hyötyä verkon todellisten tietoturvaresurssien asianmukaisessa konfiguroinnissa ja päivittämisessä.
- On myös eduksi, että houkutuslintujen avulla voidaan osoittaa, että verkon tietoturva on suunniteltu tehokkaasti.
- Houkutuslinnut auttavat tuntemaan paremmin vihollisen, sillä pelkkä tieto hakkereiden olemassaolosta ei riitä. Lisäksi on tunnettava hakkereiden tekniikat ja menetelmät. Kun hyökkääjä on saatu profiloitua, on mahdollista puolustautua uusia rikkomuksia vastaan.

(Thomas 2004, 346.)

Vaikka houkutuslinnut tarjoavat monia etuja, on niillä seuraavat rajoitukset:

- Jos järjestelmä todella hakkeroidaan, sitä voidaan käyttää astinlautana muuhun verkkoon murtautumiseen.
- Houkutuslinnut tekevät verkosta monimutkaisemman. Tietoturvassa monimutkaisuus on pahasta, koska se lisää aukkojen määrää.
- Houkutuslinnut vaativat ylläpitoa, aivan kuten kaikki muutkin verkon laitteet ja palvelut.

(Thomas 2004, 349.)

2.6 Hakkerit

Alun perin hakkereilla tarkoitettiin henkilöitä, jotka tunsivat tietokoneen toiminnan erinomaisen hyvin. Kräkkerit ovat taas hakkereita, jotka ovat keskittyneen murtamaan ohjelmien kopiointisuojauksia. Nykyään hakkereilla tarkoitetaan yleisimmin henkilöitä, jotka käyttävät tietotekniikan asiantuntemustaan haitalliseen ja todennäköisesti laittomaan toimintaan. (Ruohonen 2002, 320.)

Hakkerit jakavat itsensä kahteen joukkoon tavoitteidensa mukaan. White Hat-hakkerit pyrkivät toimimaan tietoverkkojen hyväksi ja käyttävät taitojaan rakentaviin sekä kehittäviin tarkoituksiin. Yleensä heidät esitellään mediassa erilaisina asiantuntijoina. Black Hat-hakkerit ovat edellisen vastakohta, eli he yrittävät häiritä tietojärjestelmiä ja verkkoja. Heidän tarkoituksensa on murtautua tietojärjestelmiin, levittää sekä kehittää haittaohjelmia. Media käyttää heistä nimitystä hakkeri. (Ruohonen 2002, 320.)

Hakkerit jaetaan ryhmiin myös heidän taitojensa mukaan. Script kiddiet ovat hakkereita, jotka käyttävät muiden tekemiä, käyttöjärjestelmistä ja ohjelmista löytyneitä tietoturva-aukkoja hyödyntäviä ohjelmia. Tällaisia ohjelmia löytyy Internetistä. Osa ohjelmista on voitu kehittää hyvässä tarkoituksessa verkkojen seurantaan. Näitä samoja ohjelmia voi käyttää myös vastakkaiseen tarkoitukseen. (Ruohonen 2002, 321.)

Hakkeroinnin syynä voi olla monia asioita ja tässä niistä muutamia:

- uteliaisuus
- haaste
- jännitys
- ilkivalta
- kosto
- taloudelliset syyt
- valtiolliset syyt
- aktivismi tai terrorismi
- sabotointi
- yritysvakoilu

(Ruohonen 2002, 321.)

Kannattaa muistaa, että aina vahinkojen tekijä ei ole hakkeri, hän voi olla myös työntekijä. Hän voi tehdä vahingossa tai tarkoituksella tietojärjestelmälle haitallisia asioita. Syy vahingontekoon voi olla mikä tahansa, koska olemme ihmisiä.

Sosiaalinen hakkerointi on viime aikoina kasvanut, koska se on tullut helpommaksi kuin yrittää murtautua tietojärjestelmään. Sosiaalisella hakkeroinnilla tarkoitetaan hakkeria, joka tekeytyy vaikka IT-tukihenkilöksi ja tulee pyytämään työntekijän tunnuksia käyttöön. On myös monia muita tapoja selvittää yritysten tunnuksia, kuten tutkimalla roskia ja keräämällä tietoa eri lähteistä. Tapoja on niin paljon kuin ihmisen mielikuvitus voi keksiä.

Taitava sosiaalinen hakkeri voi hankkia yksinkertaisiakin tietoja esimerkiksi: nimi, osoite, työpaikka, työntekijä numero, puhelinnumero, esimies ja käyttää näitä tietoja yhdessä jonkin muun helposti saatavilla olevan tiedon kanssa. Näin hakkeri yrittää päästä aina seuraavalle tasolle. Voidaan siis vain kuvitella, mihin verkon palveluihin hän voi päästä, jos hänellä on tiedossaan työtekijän numero, koko nimi, suora puhelinnumero töihin, osasto, työpisteen sijainti, sähköpostiosoite ja vielä esimiehen tiedot. Nämä tiedot ovat erillään harmittomia, mutta yhdistettyinä niistä tulee todellinen vaaratekijä. (Thomas 2004, 6.)

Hakkeri ei välttämättä halua mitään tietoja kohteeltaan, vaan ainoastaan saada kohteen tietokoneen tai palvelimen haltuunsa, käyttääkseen näitä hyväksi hyökätessään varsinaiseen kohteeseensa. Sen takia hakkerille käyvät myös kohteeksi kotitietokoneet, koska hän voi tarvita vaikka laskentatehoa tai käyttää kotikonetta piiloutuakseen useiden IP-osoitteiden (Internet Protocol) taakse. (Thomas 2004, 12.)

2.7 Sähköpostiuhka ja roskaposti

Suureksi ongelmaksi on muodostunut sähköpostiin tuleva roskaposti. Roskapostien välityksellä liikkuu paljon viruksia, troijalaisia, mainoksia ja muita haittaohjelmia. Tarkemmin sanottuna roskapostilla tarkoitetaan sähköpostitse tapahtuvaa massapostitusta, johon ei ole vastaanottajan lupaa. Usein lähettäjä jää hämärän peittoon tai kyseinen sähköposti- ja/tai IP-osoite on väärennetty. Suomessa roskapostin lähettäminen on pääsääntöisesti laitonta. Ainoastaan yrityksille suunnatut mainokset eivät tarvitse vastaanottajan suostumusta.

Monet Internetin tietoturvauhat leviävät lähinnä sähköpostitse. Jos tällaiset saastuneet viestit pääsevät kuitenkin livahtamaan turvaportista ja päätyvät saapuneiden sähköpostiviestien kansioon, ne voi poistaa ilman, että ongelmia aiheutuu. Tällöin saastuneet viestit on löydettävä ja poistettava avaamatta niitä tai varsinkaan liitetiedostoja.

Virustorjuntaohjelma selviytyy sähköpostiuhasta tehokkaasti sekä käyttäjien työasemissa että sähköpostipalvelimissa, jos ne on päivitetty ja asetukset on määritelty oikein. Jos yrityksellä ei ole omaa sähköpostipalvelinta, vaan käytössä on operaattorin tai muun palveluyrityksen sähköposti, on viisasta valita palvelu, joka tarkistaa kaiken liikenteen. Tämä siksi, että virukset ja roskaposti suodatetaan pois. Vaikka Internetpalveluntarjoaja käyttää virustorjuntaa, myös käyttäjien tietokoneissa on oltava virustorjunta, sillä tartunnat eivät leviä ainoastaan Internetin välityksellä vaan myös pikaviesteissä sekä ladattujen tiedostojen ja ohjelmien välityksellä. (Myhr ym. 2004, 26.)

Käytännön suojautumiskeinoina on, että ei vastaa tuntemattomiin posteihin, ei täytä tietojansa erilaisiin kyselyihin/kilpailuihin ja on aina kriittinen tuntemattomien viestien suhteen. Liitteitä ei kannata koskaan mennä avaamaan, jos ei tiedä lähettäjää ja sähköpostista ei selviä, mitä liite pitää sisällään.

Suodatinohjelmat ovat yksi tapa suojautua roskapostilta. Bayesilainen roskapostisuodatus menetelmä on suosittu ja erinomainen käyt-

tää, koska sen, sekä vastaavat ohjelmat voi itse opettaa suodattamaan haluamiansa posteja. Niiden toimintaperiaate on, että aluksi käyttäjä kertoo niille mitkä sähköpostit ovat roskapostia. Suodatin oppii nopeasti tekemään erottelun tehokkaasti. Esimerkiksi Mozilla Thunderbird -sähköpostiohjelma sisältää tällaisen suodatusohjelman.

Internetistä on myös saatavilla estolistoja, joita voi hyödyntää suodatukseen. Kannattaa kuitenkin muistaa, että liian raju suodatus alkaa nopeasti karsimaan oikeitakin viestejä. Sähköpostipalvelimille voi myös asentaa suodatuksia, jotka poistavat automaattisesti roskaposteja. Yleensä käyttäjälle luodaan oma kansio roskapostille, joka kannattaa tarkistaa ennen tuhoamista, sillä oikeitakin sähköposteja voi joutua roskapostin joukkoon.

2.8 Palvelinhuone

Pienehkössä toimistossa tietoliikenneympäristö on usein melko tyypillinen: pienessä palvelinhuoneessa on muutamia palvelimia, joista yksi huolehtii tiedostojen tallentamisesta ja yhteisistä sovelluksista, toinen sähköpostista ja kolmas internet-sivustosta. Tiedostopalvelimeen on yhdistetty UPS-virtalähde (Uninterrupted Power Supply) huolehtimaan sähkönsyötöstä häiriötilanteissa. Tärkeimmät tietoliikennelaitteet sijaitsevat usein samassa paikassa, kuten reititin Internet-yhteyttä ja muuta ulkoista tietoliikennettä varten. lähiverkon kytkin, palomuuri ja mahdollisesti verkon suojausjärjestelmä. (Myhr ym. 2004, 12.)

Tietokone- tai palvelinhuone sisältää toimiston tärkeimmän tietotekniikkajärjestelmän. Sen kautta kulkee ja siellä säilytetään suuria määriä tärkeää tietoa, siksi fyysiseen suojaamiseen on kiinnitettävä huomiota. Tietokone- tai palvelinhuoneen oven on oltava lukittu ja vastaavasti pienemmissä toimistoissa kaapin ovi. Huonetta tai kaappia ei saa käyttää muihin tarkoituksiin. Sinne saavat mennä yksin vain vastuuhenkilöt, joiden työtehtävät edellyttävät tätä. Suojausta voi lisätä tietokonehuoneen siivoaminen valvotusti sen sijasta, että se siivottaisiin iltaisin muiden tilojen siivoamisen yhteydessä. Vastuuhenkilöt voivat hoitaa myös siivouksen itse. (Myhr ym. 2004, 13.)

2.9 Lähiverkko

Suunnitellessa lähiverkkoa yrityksen tiloihin kannattaa miettiä tarkkaan, mihin eri laitteet voidaan sijoittaa. Tämä jo pelkästään sen takia, että johtoja ei kulkisi pitkin lattioita. On hyvä piirtää pohjapiirustus, josta näkee missä eri laitteet sijaitsevat. Tämä voi tuntua turhalta yhden tai muutaman hengen yrityksessä, mutta se hel-

pottaa asentajien työtä ja tulevaisuudessa mahdollisen vian etsimistä.

Tietoturvan parantamiseksi on hyvä, että mahdolliset modeemit, reitittimet, kytkimet, palomuuri jne. sijaitsevat samassa paikassa, mielellään lukkojen takana. Pienessä yrityksessä yleensä nämä kaikki laitteet/ominaisuudet ovat samassa fyysisessä laitteessa. Tähän kyseiseen tilaan tai kaappiin olisi hyvä myös sijoittaa mahdolliset backup-laitteet.

Pienen yrityksen verkko yleensä koostuu ADSL-modeemista (Asymmetric Digital Subscriber Line), (jossa on reititin, kytkin ja palomuuri samassa laitteessa, ehkä vielä WLAN-tukiasemakin) parista tietokoneesta ja tulostimesta. Tällainen verkko on helppo toteuttaa, mutta se ei tarkoita sitä, että tietoturva-asioita voisi ottaa vähemmän huomioon kuin isoissa yrityksissä, joissa on laajemmat verkot.

Reitittimen asetuksissa tulisi ottaa huomioon, ettei siihen saa kytkettyä muita koneita kuin yrityksen omat. Sama koskee langatonta verkkoa eli asetukset on määriteltävä tarkkaan. On tärkeää, että kukaan ei voi tuoda vierasta konetta verkkoon tai ottaa langattomaan verkkoon yhteyttä ilman lupaa, koska kyseinen henkilö voi varastaa tietoja tai aiheuttaa vahinkoa muuten yrityksen tietojärjestelmälle eli lähiverkolle.

Verkko on siis toteutettava siten, että siihen ei pysty kytkemään vierasta konetta. Tämä voidaan toteuttaa verkon asetuksilla. Yrityksen verkkoon asetetaan oikeudet sen omille koneille MAC-osoitteiden (Media Access Control address) perusteella. Jokaisella laitteella on oma MAC-osoitteensa, jolla se voidaan erottaa muista laitteista. Yrityksen henkilöstölle annetaan käyttäjäprofiilit, joilla he pääsevät verkkoon ja samoilla tunnuksilla he pääsevät kirjautumaan tietokoneille. Ilman luotua profiilia henkilö ei pääse verkkoon tai tietokoneisiin käsiksi.

Langattomaan verkkoon asetetaan myös vastaavat suojaukset ja asetukset kuin varsinaiseen verkkoon. Tästä lisää seuraavassa alaluvussa, jossa käsitellään langattomia verkkoja.

Laitteet kannattaa hankkia pitäen silmällä mahdollista verkon laajentamista. Tämä siksi, että jos tarvitsee lisätä kaksi tietokonetta lisää lähiverkkoon, niin ei tarvitse hankkia hankia uutta reititintä tai uusia verkkolaitteita.

2.10 WLAN-verkko

Tekniikan kehittyessä on tullut yleiseksi asentaa WLAN-tukiasemia (Wireless Local Area Network) koteihin ja yrityksiin. Tämä on kasvattanut uhkien määrää ja näin ollen lisännyt tietoturvan tarvetta. Kannattaa huomioida, että tekniikan lisääntyessä lisääntyy myös riskien määrä.

Langaton lähiverkko antaa vapauden liikkua toimistossa ja helpottaa esimerkiksi kannettavien käyttöä. Samalla, kuten aikaisemmin jo mainittiin, se lisää lähiverkon haavoittuvuutta. Tämän takia WLAN-tukiaseman asetukset tulee määritellä tarkkaan. Emme halua, että naapurit käyttävät verkkoamme tai tutkivat verkon liikennettä. Pahimmassa tapauksessa he pääsevät näkemään tiedostomme tai aiheuttamaan vahinkoa tietojärjestelmään.

Moni innokas tietokoneharrastaja voi mielenkiinnosta yrittää saada yhteyden vieraaseen lähiverkkoon. He eivät välttämättä halua tehdä vahinkoa, mutta on kuitenkin olemassa hakkereita ja ihmisiä, jotka sitä haluavat tehdä. On olemassa myös haittaohjelmia, jotka voivat tarttua suojaamattoman langattoman verkon kautta.

Langattomien verkkojen tultua on kehittynyt tapoja, joita hakkerit käyttävät löytääkseen langattomia verkkoja. WarChalking, WarSpying, WarSpamming ja WarDriving ovat yksikertaisesti termejä, joita hyökkääjät käyttävät kuvatakseen toimintaansa. WarChalkingin tarkoitus on ilmoittaa muille ihmisille, missä on ilmaisia ja suojaamattomia langattomia verkkoja. WarSpying on uusi ilmiö, jossa on kyse langattomien videoverkostojen vakoilemisesta. Tarkoitus on siepata langattomien valvontajärjestelmien liikennettä. WarSpamming on sanan mukaisesti roskapostin lähettämistä langattomien verkkojen välityksellä. WarDriving:lla tarkoitetaan henkilöä, joka etsii autolla langattomia verkkoja. Hänellä on autossa laitteet, joilla hän pystyy skannaamaan aluetta liikkuessaan. (Thomas 2004, 289.)

Langattoman tukiaseman SSID (Service Set Identifier eli tukiasemalle annettava ainutkertainen nimi) tulisi konfiguroida vaikeasti arvattavaksi, niin että sen nimi ei muistuta tai viittaa mitenkään kohteeseen (esimerkiksi yritykseen, paikkaan). Tukiasema lähettää oletusarvoisesti SSID:n muutaman sekunnin välein majakkaviestinä. Tämän takia valtuutettujen käyttäjien on helpompi löytää oikea verkko. Tosin samalla myös valtuuttamattomat käyttäjät löytävät verkon. SSID-yleislähetys kannattaa kytkeä pois päältä aivan ensimmäiseksi. (Thomas 2004, 303.)

Seuraavaksi konfiguroidaan tukiasemalle MAC-osoitesuodatus (Media Access Control addres). Verkkokortin MAC-osoite on 12-

numeroinen heksadesimaaliluku, joka on yksilöllinen jokaisella maailman verkkokortilla. Koska jokaisella langattomalla Ethernet-kortilla on yksilöllinen MAC-osoitteensa, voidaan verkosta sulkea kaikki siihen kuulumattomat, jos tukiasema rajoitetaan vain luvallisten laitteiden MAC-osoitteille. (Thomas 2004, 307.)

MAC-osoitesuodatus ei kuitenkaan ole täysin turvallinen, ja siksi siihen ei kannata ainoastaan luottaa. Kannattaa ottaa huomioon, että MAC-osoitteita voidaan muuttaa. Joten päättäväinen hyökkääjä voi käyttää langatonta nuuskintaa selvittääkseen sallitun MAC-osoitteen ja asettaa PC:nsä vastaamaan luvallisia asetuksia.

Langattomaan tukiasemaan tulee ottaa käyttöön autentikointi (todennus eli käyttäjän identiteetin varmistaminen) ja salausprotokollat. Yleisiä autentikointimenetelmiä on WEP (Wired Equivalent Privacy), WPA (Wireless Fidelity Protected Access), EAP (Extensible Authentication Protocol), (joista löytyy useampi vaihtoehto) ja WPA2. Salausprotokollissa yleisimpiä on WEP, WPA(TKIP, Temporal Key Integrity Protocol), WPA2(AES, Advanced Encryption Standard). Toisella varmistetaan siis oikea käyttäjä ja salausprotokollalla salataan langaton liikenne.

WEP-protokollan tarkoitus on estää kaikista yksinkertaisimmat hyökkäysyritykset langattomaan verkkoon. Tänä päivänä WEP-protokollan murtaminen kestää muutamia minuutteja ammattilaiselta. Näin ollen kannattaa mieluummin käyttää WPA-salausta. WPA käyttää 128-bittistä pakettikohtaista salausavainta. WPA sisältää pakettien eheyttä valvovan MIC (Message Integrity Check)-toiminnon, joka varmistaa jokaisen paketin, että mahdollinen hyökkääjä ei ole ottanut paketteja ja muuttanut niiden tietoja.

Langatonta tietoturvaa voidaan parantaa monilla keinoilla, mutta myös langattomien lähiverkkojen sudenkuopat ovat saaneet runsaasti huomiota. Sen takia monet organisaatiot ovat kieltäneet kokonaan langattomat lähiverkot. Turvallisuustietoiset organisaatiot kuitenkin linnoittavat WLANinsa kerrosteisella tietoturvalla, joka sisältää seuraavia keinoja:

- Langaton verkko sijoitetaan oman reititinliityntänsä taakse, jolloin yhteys voidaan tarpeen vaatiessa estää yhdessä kuristinpisteessä.
- Rosvotukiasemien ja niihin liittyvien mahdollisten haavoittuvuuksien estäminen.
- Tukiasemien fyysisellä ja loogisella tietoturvalla varmistetaan, ettei kukaan voi havaitsematta mennä tukiaseman luokse muuttamaan sen konfiguraatiota.
- SSID:n muuttaminen ja satunnaisesti luodun SSID:n käyttö, jolloin yrityksessä tai verkosta ei voi saada mitään tietoa.

- SSID-yleislähetyksen kytkeminen pois päältä.
- Yleislähetysavainten kierrätys vähintään kymmenen minuutin välein.
- Salaus ja todennus, joihin saattaa sisältyä langattomassa verkossa toteutettu VPN (Virtual Private Network).
- Tarjolla oleviin salauksiin tutustuminen ja oman vaihtoehdon valitseminen.
- Langattoman verkon tietoturvakäytäntöjen luominen ja toimeenpano.
- Ennakoivien turvatoimenpiteiden, kuten tunkeutumisen eston käyttöönotto.
- Langattoman tukiaseman ei tulisi jakaa ylimääräisiä IP-osoitteita, vaan ainoastaan yrityksen tarvitsema määrä.

(Thomas 2004, 311.)

WLAN-verkkoon liitetyt tietokoneet kannattaa suojata erillisillä palomuureilla. Tämä sen takia, että varsinainen palomuuri, joka sijaitsee Internetin ja lähiverkon välillä ei suojaa langattomilta hyökkäyksiltä. Kannettavia tulee käytettyä eri paikoissa, joten ne altistuvat huomattavasti helpommin hyökkäyksille. Kaikki tietoturvaa parantavat ohjelmat (virustorjunta, anti-spyware ohjelmat jne.) ja oma henkilökohtainen käytös tulee huomioida liikuttaessa työpaikan ulkopuolella.

Kannettaviin tietokoneisiin tulee asettaa BIOS (Basic Input-Output System)-salasana ja lisäksi myös käyttöjärjestelmän oma salasana. Näin tietoturva parantuu väärinkäytösten varalta, jos kone esimerkiksi jätetään yleiseen tilaan (lukittu kaikkien poistuessa) esimerkiksi kokoustaukojen aikana. Kannattaa myös säätää näytönsäästäjä lyhyelle viiveelle ja ottaa siihen käyttöön salasana. Tietokoneet kannattaa muutenkin aina lukita, kun poistutaan niiden läheisyydestä, myös työpaikalla. Varkaustilanteiden varalta olisi hyvä, että kaikki tärkeät tiedostot olisivat kryptattuja.

Paras tapa tietoturvan kannalta langattoman verkon toteuttamiseksi olisi, että langallinen ja langaton verkko olisivat erillisiä. Tällä tavalla yrityksen varsinainen (johdoilla toteutettu) lähiverkko on huomattavasti turvallisempi. Yhteydet langattomasta verkosta varsinaiseen yrityksen verkkoon toteutetaan VPN-yhteyksillä palomuurin kautta.

2.11 Etäyhteydet

Etäyhteyksiä tarvitaan, jotta käyttäjät voisivat toimia ja tehdä töitä paikasta riippumatta. Erilaisilla etäyhteyksillä mahdollistetaan käyttäjälle yrityksen resurssit, jotka ovat tietoverkossa. Tiedostoi-

hin voi päästä käsiksi mistä päin maailmaa tahansa, jos on käytössä internet. Siis jos tarvitset toimistolla olevasta työkoneestasi dokumentin, voit sen etäyhteydellä hakea kannettavaasi.

Etäyhteys kannattaa aina suojata ja siksi käytetään salausprotokollia. Salausprotokollilla voidaan muodostaa suojattuja yhteyksiä. Niillä voidaan varmistaa, että mikään suojatulla yhteydellä lähetetty viesti ei ole muuttunut matkalla lähettäjältä vastaanottajalle, viestit ovat suojatun yhteyden toisen osapuolen lähettämiä ja/tai salakirjoittaa viestien sisällön. Salausprotokollat käyttävät usein tunnistus-, avaimensopimis- ja/tai avaintenjakoprotokollia. Kahden tietokoneen välillä oleva yhteys voidaan tarvittaessa suojata tavallisella salausprotokollan yhteydellä, kun taas kahden verkon välillä oleva yhteys täytyy suojata tunnelilla. (Ruohonen 2002, 96.)

Monilla yrityksillä on vieläkin käytössä vuokralinjoja tai frame relaylla toteutetuista yksityisistä yhteyksistä. Nykyään turvallinen yhteys pystytään toteuttamaan VPN-verkoilla. VPN-verkot mahdollistavat etäyhteydet myös pienille yrityksille, koska kustannukset eivät ole suuret.

Yhteyksiä voi muodostaa monella eri tavalla ja erilaisilla ohjelmilla riippuen käyttötarkoituksesta. Seuraavaksi aion esitellä pari hyvää vaihtoehtoa etäyhteyden muodostamiseen, tutustuminen muihin vaihtoehtoihin on myös suotavaa.

2.11.1 SSH

Secure Shell eli yleisimmin SSH protokolla on yksi hyvä tapa kirjautua etätietokoneeseen. SSH toimii paljolti samalla tavalla kuin Telnet. Ero syntyy siinä, että SSH tarjoaa yhteydelle huomattavasti paremman tietoturvan. SSH on ohjelma, joka tarjoaa kahden tietokoneen välille salatun tiedonsiirtopolun, mahdollisen turvattoman verkon yli. (Thomas 2004, 145.)

Yleensä SSH:ta käytetään etäkirjautumiseen, mutta protokollaa voidaan käyttää yleiskäyttöisenä salaustunnelina, joka pystyy kopioimaan tiedostoja, salaamaan sähköpostiyhteyksiä ja käynnistämään ohjelmia etäyhteyden yli. SSH:lla voidaan siis muodostaa kahden tietokoneen välille yhteys verkon yli salattuna. SSH toimii omana ohjelmanaan sekä työasemassa että palvelimessa, joten SSH-yhteyden avaaminen palvelimeen tai toiseen koneeseen tehdään käynnistämällä SSH-asiakasohjelma, joka avaa yhteyden palvelimessa/tietokoneessa käynnissä olevaan SSH-palvelinohjelmaan. (Ruohonen 2002, 287.)

Yksinkertaisimmillaan SSH muodostaa TCP-yhteyden (Transmission Control Protocol) isäntään ja todentaa käyttäjätunnusta ja salasanaa käyttämällä. Kun todennus on onnistunut, SSH aloittaa datan eli tiedon salauksen. (Thomas 2004, 149.) SSH:ta on kaksi versiota, joista ensimmäisessä (SSH1) oli useita virheitä sekä ongelmia, joten kannattaa käyttää uudempaa versiota (SSH2), jos on mahdollista. SSH ei auta suojaamaan sisäisiä järjestelmiä. (Thomas 2004, 145.)

2.11.2 VPN

Virtuaalinen yksityisverkko (VPN, Virtual Private Network) on keino muodostaa salattu verkkoyhteys haluttuun kohteeseen. Kohteiden välille muodostetaan tunneli Internetin tai muun verkon kautta. VPN-verkko on siis julkisen verkon sisällä toimiva suojattu verkko. Tarkoituksena on käyttää olemassa olevaa julkista verkkoa (Internet) siten, että vain suojattuun verkkoon kuuluvat tietokoneet voivat lähettää ja vastaanottaa verkkoon osoitettuja viestejä. (Ruohonen 2002, 95.) Parhaiten tietotekniikkapalveluiden tarjoaminen turvallisesti ja järkevällä tavalla paikasta riippumatta onnistuu Internet Protocol Security Protocol- eli IPSec-protokollalla salatuin virtuaalisin yksityisverkoin (VPN) (Thomas 2004, 231).

IPSec (IP security) on salausprotokolla, joka mahdollistaa:

- viestien eheyden varmistamisen (varmistaa ettei viesti ole muuttunut matkalla)
- viestien lähettäjän varmistaminen
- viestien toistamisen estämisen
- viestien salakirjoittamisen

(Ruohonen 2002, 291.)

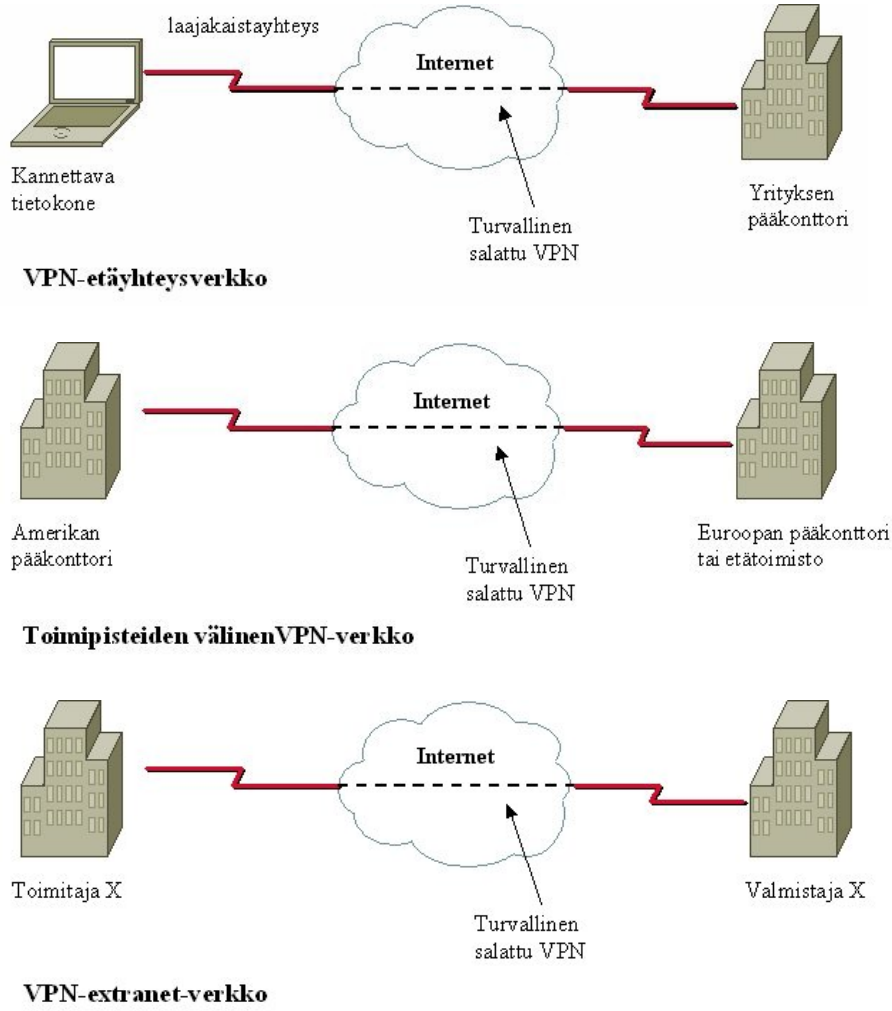
VPN-verkon muodostamiseksi kahden eri verkon välille tulee molempiin verkkoihin asentaa VPN-yhdyskäytävä (VPN gateway), jotka avaavat välilleen yhteyden salausprotokollalla. Tämän jälkeen yhdyskäytävät tunneloivat kaikki niiden kautta kulkevat – toisen VPN-yhdyskätävän verkkoon matkalla olevat – paketit tämän yhteyden kautta. VPN-yhdyskäytävä voi toimia joko omana laitteenaan, osana palomuuria tai tietokoneessa (jossa on kaksi verkkokorttia). (Ruohonen 2002, 95.)
VPN-verkkoja on kolmea päätyyppiä, jotka on hyvä tietää. Nämä antavat hieman käsitystä mistä on kyse:

- **VPN-etäyhteysverkot** – Yksittäiset yhteyksien käyttäjät voivat muodostaa turvallisen yhteyden esimerkiksi toimistoon Internetin kautta. Kysymyksessä on yhteys, jolla työn-

tekijä pääsee yrityksen lähiverkkoon käsiksi kentältä. Heidän järjestelmissään on VPN-asiakasohjelma, joka tekee mahdolliseksi turvallisen linkin heidän ja yrityksen lähiverkon välille.

- **Toimipisteiden väliset VPN-verkot** – Olemassa oleva lähiverkko laajennetaan muihin rakennuksiin tai toimipisteisiin erillislaitteita käyttämällä. Tällä tavalla eri paikoissa työskentelevä henkilö/henkilöstö voi käyttää samoja verkkopalveluja. Nämä VPN-verkot ovat aktiivisesti päällä kaiken aikaa.
- **VPN-extranet-verkot** – Nämä verkot tekevät mahdolliseksi turvallisen sähköisen kaupankäynnin liikekumppanien, toimittajien ja asiakkaiden kanssa. VPN-extranet-verkot ovat VPN-intranet-verkkojen laajennus, jossa sisäinen verkko suojataan palomuurein.

(Thomas 2004, 238.)



Kuva 1. VPN-Verkkojen tyypit (Thomas 2004, 238).

Yhteyden saamiseksi ja toimimiseksi hyvin salattuna IPSec käyttää kolmea toisiaan täydentävää protokollaa. Nämä protokollat yhdessä käytettynä muodostavat yhtenäisen ja turvallisen, standardien mukaisen kehyksen, joka sopii erinomaisesti VPN-verkkoihin. IPSec-standardeissa on kuvattu kolme seuraavaa protokollaa:

- Internet Security Association Key Management Protocol (ISAKMP) – Kuvaa vaiheen, jossa IPSec-yhteys neuvotellaan VPN:n muodostamiseksi. Ennen suojatun tunnelin muodostamista kohteiden pitää määritellä menetelmä todennetun aivaintenvaihdon suorittamiseksi eli toistensa todentamiseksi.
- Encapsulated Security Protocol (ESP) – Tarjoaa datan luotettavuuden ja suojauksen valinnaiselle todennukselle ja uudelleensoiton havaitsemispalveluille.

- Authentication Header (AH) – Tarjoaa todennuksen ja uudelleensoiton estopalvelut (valinnainen).

(Thomas 2004, 250.)

Edellä kuvatut asiat ovat osa suojatun yhteyden muodostamiseen vaadittavia toimia. Käyttäjän ei välttämättä näistä tarvitse tietää. Nykyään palomuureista, reitittimistä, palvelimista ja tietokoneista. löytyvät valmiit ohjelmat, jotka muodostavat VPN-yhteyden. Pitää vain tietää tarvittavat tunnukset ja salasanat. Kannattaa tiedustella, miten omilla laitteilla kyseiset käytännöt toimivat.

On kuitenkin hyvä olla jonkunlainen käsitys siitä, miten VPN-yhteys toimii. Yksinkertaisesti kuvattuna yhteyden muodostuttua kaikki tieto kulkee salattuna (kuvainnollisesti) tunnelia pitkin. Kummankin kohteen koneet purkavat tiedot sovituilla menetelmillä ymmärrettävään muotoon.

2.12 Varmuuskopiointi

Nykyään suuri osa yrityksen dokumenteista, tiedoista ja toimintaan liittyvistä materiaaleista on sähköisessä muodossa tietokoneilla. Nämä tietokoneen kovalevyllä sijaitsevat tiedot ovat usein elintärkeitä yrityksen toiminnalle. Voidaan vain kuvitella miten käy, jos kyseiset tiedot tuhoutuisivat. On siis syytä varmistaa, että nämä tiedot ovat yrityksellä käytettävissä, ja siksi on otettava varmuuskopiot tiedostoista.

Varmuuskopioiminen on tietoturvan perusta. Se on yksinkertaista ja edullista. Verkkopalvelimessa on aina paikka varmuuskopiointiyksikölle. Siihen voi kopioida tietoja palvelimen kiintolevystä sekä käyttäjien tietokoneista lähiverkon kautta. Varmuuskopiointiyksikkönä käytetään monenlaisia laitteita, esimerkiksi: nauha-asemaa, DVD:tä, CD:tä, muistitikkua ja kovalevyjä.

Nauha-asemalla tiedot tallennetaan kaseteille. Nykyään keskisegmentiin kuuluu Super DLT-tekniikka (DLT, Digital Linear Tape), yhdelle nauhalle saadaan mahtumaan jopa 800 Gigaa dataa. AIT-formaatti (Advanced Intelligent Tape) on Sonyn julkaisema tekniikka. Tällä hetkellä AIT-5 tarjoaa n. 400 gigatavua tallenuskapasiteettia, siirtonopeudella 24 Mb/s. Vativimpiin tarkoituksiin Sony:lta löytyy S-AIT-formaatti, joka oli ensimmäisiä formaatteja, joka pystyy tallentamaan yli teratavun tietoa (pakattuna) yhdelle kasetille. (Wikipedia 2007.) LTO-tekniikka (Linear Tape-Open) on HP:n, IBM:n ja Seagate:n yhdessä kehittämä, sen tunnetuin versio on Ultrium-formaatti. Tallennus kapasiteettia löytyy (LTO-4) 800 gigatavua ja tiedonsiirtonopeudet ovat n. 120 Mb/s. (Wikipedia

2007.) Vaativimpiin tarpeisiin on kehitetty myös nauharobotteja, jotka vaihtavat useita kasetteja automaattisesti (Myhr ym. 2004, 41).

CD-ROM- ja DVD-levyt riittävät vaatimattomimpiin tarpeisiin. Yksinkertaisimmissakin henkilökohtaisissa tietokoneissa on nykyään tallentava CD- tai DVD-asema. Ne soveltuvat hyvin omien ja joskus myös pienehkön yrityksen tietojen varmuuskopiointiin. On kuitenkin muistettava, että itse tallennetut CD- ja DVD-levyt ovat varsin arkoja. Niiden tallennuspintaa ei nimittäin suojaa lakkakerros, toisin kuin valmiiksi tallennettujen levyjen. Tavallinen vesijohtovesi voi tuhota pinnan. (Myhr ym. 2004, 41.) Yksi tapa varmistaa tietokoneen kovalevyllä olevat tiedot on peilata kovalevy. Windows XP:ssä peilauksen saa toteutettua helposti Disk Management:n kautta. Kovalevyn peilauksella varmistetaan, että tietoja ei menetetä vikatilanteissa. Peilattu kovalevy on sisällöltään identinen käytössä olevan levyn kanssa.

Yrityksissä, joissa on palvelin käytössä, kannattaa palvelin asettaa suorittamaan varmuuskopiointi päivittäin. Palvelin voi tarvittaessa ajaa varmuuskopioinnin ulkoiselle kovalevylle tai mahdolliselle toiselle palvelimelle, joka sijaitsee toisessa osoitteessa.

Varmuuskopiot tulisi säilyttää paloturvakaapissa tai eri osoitteessa kuin varsinaiset yrityksen tiedostot. Tällä varmistetaan tietojen säilyminen esimerkiksi tulipalon sattuessa. Jos ei halua investoida omaan paloturvakaappiin, niin varmuuskopiolle kannattaa vaikka hankkia pankista turvalokero, jonne kerran kuukaudessa vie varmenteen. Kopioinnit tulisi suorittaa tarvittavan usein, niin että vahingon sattuessa vahingot olisivat mahdollisimman pienet. Varmuuskopioinnin voi ajastaa tapahtuvaksi vaikka jokaisena iltana.

Katastrofilta suojautuminen edellyttää, että varmuuskopiointi on kunnossa. Ei riitä, että varmuuskopiot otetaan säännöllisesti. Lisäksi tietojen palauttaminen varmuuskopioilta on testattava. Järjestelmän sisältö voidaan palauttaa helpommin käyttämällä erityistä tiedostojen kuvaa. Tällöin kiintolevyn koko sisältö varmuuskopioidaan. Kriisitilanteessa säästyy paljon aikaa, kun järjestelmä palautetaan tämän kopion avulla eikä kaikkia ohjelmia tarvitse asentaa uudelleen alusta alkaen. (Myhr ym. 2004, 34.)

Yritys voi lisäksi ulkoistaa tärkeiden järjestelmien käytön. jolloin omissa tiloissa on tärkeistä tietokoneista ja tiedostoista mahdollisimman pieni osa. Pienen yrityksen kannattaa ostaa WWW- ja sähköpostipalvelin operaattorilta, WWW-hotellista tai konsulttiyritykseltä. Yhä useammat tietotekniset järjestelmät voi vuokrata. Näistä uusilla palvelumarkkinoilla vaikuttavista toimittajista käytetään nimitystä ASP (lyhenne sanoista Application Service Provider). Ne

tarjoavat laajan palveluvalikoiman esimerkiksi taloushallintoon, asiakassuhteiden hoitoon ja palkanlaskentaan. (Myhr ym. 2004, 35.)

Varmuuskopiointiratkaisun laatu määräytyy harvoin tekniikan mukaan. Suorituskyvyllä on merkitystä vain silloin, jos käytettävyydelle asetetaan poikkeuksellisen suuret vaatimukset tai tietojen määrä on hyvin suuri suhteessa yrityksen kokoon. Tärkeintä on ottaa kattavat varmuuskopiot tiedoista. (Myhr ym. 2004, 39.) Tämä helpottaa tietojärjestelmän uudelleen pystyttämistä vikatilanteessa.

2.13 Laitteistot

Markkinoilta löytyy monenlaisia hyödyllisiä laitteita, joilla voidaan varmistaa ja parantaa tietojärjestelmien tietoturvallisuutta. Nämä laitteet eivät ole kalliita edes pienelle yritykselle, ja kannattaa muistaa aina, mitä voi tapahtua ilman suojautumista uhkia vastaan.

2.13.1 Keskeytymätön virransyöttö ja varavoima

UPS (Uninterrupted Power Supply) syöttää virtaa sähkökatkoksen aikana. Ainakin kaikissa palvelimissa tulee olla UPS-laite. Se suojaa järjestelmää ja tietoja sähkökatkosten aikana. Laitteen akuissa riittää virtaa palvelimelle. Perustason UPS-laitteessa on virtaa 30 minuutiksi. Tämä aika riittää palvelimen sammuttamiseen hallitusti. Jos virran täytyy riittää pidemmäksi ajaksi, on hankittava suurempi varavirtalaite.

UPS-laite on eri asia kuin varavoimala, joka tuottaa tietokoneille virtaa jatkuvasti koko sähkökatkoksen ajan. Tällaisessa laitteessa on dieselgeneraattori. Nämä laitteet ovat kalliita, ja niitä käytetään vain suurissa tietokonekeskuksissa. UPS-laite soveltuu useimmille yrityksille. Niiden hinnat alkavat noin sadasta eurosta. (Myhr ym. 2004, 39.)

Ylijännitesuoja on hyvä olla suojaamassa kaikkia sähkölaitteita mahdollisilta virtapiikeiltä. Nykyään myydään jakorasioita, joissa on integroituna ylijännitesuoja. Salamaniskut ja jännitepiikit voivat aiheuttaa huomattavia vaurioita elektronisille laitteille, kuten tietokoneille, tulostimille jne. Jännitteen vaihtelut ja virran epäpuhtaudet voivat saada aikaan tietokoneen lukkiutumisen tai tiedostojen katoamisen. Ylijännitesuoja/jakorasiat on suunniteltu suojaamaan tällaisilta ongelmilta, niissä on usein myös vakuutukset kyseisten kaltaisten vahinkojen sattuessa laitteille. Nykyään löytyy myös ylijännitesuojan/jakorasian ja UPS:n yhdistelmiä eli samassa laitteessa kumpikin.

2.13.2 Ylläpito

Pienessä yrityksessä on harvemmin IT-henkilöitä jotka hoitavat ylläpidollisia tehtäviä, joten kannattaa nimetä henkilö, joka on vastuussa asiasta. Laitteet tarvitsevat myös ylläpidollisia toimenpiteitä siinä missä ohjelmiakin päivitetään. Tietokoneen eri komponenteille löytyy ajureita, joita kannattaa päivittää, kun niihin tulee päivityksiä. Sama koskee palvelimia ja reitittimiä. Näin laitteet toimivat paremmin ja ovat tietoturvan kannalta toimivimpia.

Ohjelmistot kannattaa päivittää mahdollisimman usein, etenkin tietoturvaan liittyvät ohjelmat. Virustorjunta-, palomuuri- ja antispyware ohjelmistot kannattaa säätää automaattisesti päivittyviksi. Kannattaa tietenkin tehdä muitakin toimenpiteitä, kuten tietokoneen kovalevyn defragmentointi eli eheyttäminen aika ajoin. Tämä nopeuttaa kovalevyn tiedonhakemista.

2.13.3 Vanhojen laitteiden hävittäminen

Vanhoja tietokoneita hävittäessä kannattaa olla tarkkana. Vanhalla kovalevyllä voi olla yritykselle tärkeitä tietoja tai muuten henkilökohtaisia tietoja. Pelkkä formatointi ei riitä tietojen pyyhkimiseen, vaan vanha kovalevy täytyisi kirjoittaa täyteen turhaa tietoa. Tämä siksi, että tieto jää kovalevyn pintaan. Toisin sanoen vanhat tiedot eivät tuhoudu kovalevyltä muuten kuin ylikirjoittamalla.

Nykyään löytyy markkinoilta monia helppokäyttöisiä tiedonpalautusohjelmistoja, joita voi kuka tahansa hankkia. Näin voi halutessaan tutkia vanhoja kovalevyjä ja palauttaa tärkeitä tietoja käyttöönsä. Kannattaa muistaa, mitä hakkeri voi tällaisella tiedolla tehdä. Vaikka tiedostot olisi kryptattuja, niin ne voidaan saada selville.

Markkinoilta löytyy monia tiedonhävitysohjelmia, joilla voidaan ylikirjoittaa vanhat tiedot. Näiden ohjelmien ostamisen kanssa kannattaa kuitenkin olla tarkkana, koska markkinoilla on sellaisiakin ohjelmia, joiden jäljiltä on testeissä löydetty tietoja. Ohjelmat eivät ole hirveän kalliita, varsinkaan suhteutettuna siihen, mitä kovalevyillä olevat tiedot voivat aiheuttaa väärissä käsissä. Isommille yrityksille tietojen tuhoaminen ohjelmistoilla on tärkeätä, koska tietokoneita ja palvelimia vaihdetaan usein. (Kirves 2007.)

Kiintolevy voidaan tuhota myös fyysisesti hajottamalla se kappaleiksi, jolloin siitä ei enää voida saada dataa. Toinen keino on demagnetointi, millä tarkoitetaan kiintolevyn tai tallentamislaitteen altistamista suurtehomagneetille. Näin laitteen magneettivaraukset, jotka tulkitaan biteiksi, saadaan sekoitetuksi. Tämä aiheuttaa sen,

että tiedon luku laitteelta on mahdotonta. Demagnetoitu levy on käyttökelvoton, joten siitä tulee ongelmajätettä.

Käytettäessä tiedostoja ylipyyhkivää ohjelmaa kannattaa muistaa, että se pyyhkii pois kaikki tiedot, käyttöjärjestelmiä myöden. Pyyhinnän jälkeen kovalevylle on asennettava uusiksi käyttöjärjestelmä, jos on tarvetta. (Kirves 2007.)

2.14 Salasanat

Salasanat ovat tärkeä osa tietojärjestelmien tietosuojaa. Henkilökohtaisia salasanoja ei saa luovuttaa kenellekään (riippumatta henkilöiden asemasta yrityksessä), ne ovat aina henkilökohtaisia. Yksikään ammattilainen ja tietojärjestelmiä hoitava ei niitä tule kysymään, ja jos joku vaatii tietoonsa toisen salasanoja, on tästä ilmoitettava välittömästi tietoturvasta vastaavalle yksikölle tai henkilölle.

Salasanat tulisi vaihtaa säännöllisesti, koska käyttäjien salasanat ovat ensimmäinen asia, jonka hyökkääjä yrittää murtaa (Thomas 2004, 161). Useimmissa järjestelmissä pystyy asettamaan automaattisen muistutuksen salasanan vaihdosta määrätyn ajan kuluttua. Kaikki järjestelmätason salasanat tulee vaihtaa neljännesvuosittain. Käyttäjätason salasanat (esimerkiksi sähköposti, web, työasema jne.) tulisi myös vaihtaa noin neljän kuukauden välein.

Järjestelmätason oikeuksilla olevilla käyttäjätileillä on oltava eri salasanat, kuin kyseisten käyttäjien muilla tileillä. Salasanoja ei saa koskaan tallentaa tietokoneelle (Word, Notepad), sisällyttää sähköpostiviesteihin tai muihin sähköisessä muodossa tapahtuvaan viestintään. Salasanoja ei olisi suotavaa kirjoittaa edes paperille muistiin. Paras olisi keksiä sellainen salasana, jonka muistaa ulkoa. Salasanaa ei koskaan saa luovuttaa kenellekään, vaan tarvittaessa luoda omat salasanat muille ohjelmia käyttäville henkilöille.

On tärkeää, että salasana sisältää useita merkkejä. Koskaan ei saisi käyttää salasanaa joka on selkeä sana, nimi, laulu, yksinkertainen numerosarja jne.

Huonoilla, heikoilla salasanoilla on seuraavia piirteitä:

- Salasanassa on alle kahdeksan merkkiä
- Salasana on löydettävissä sanakirjasta (suomen- tai muunkielisestä)
- Salasana on yleisesti käytössä oleva sana, kuten:
    - Perheen, lemmikkieläimen, ystävän, työtoverin, mielikuvitushahmon tai vastaavan nimi.

- Tietokoneentermi tai tietokoneen nimi, komento, verkko, yritys, laitteisto, ohjelmisto.
- Syntymäpäivä tai muu henkilökohtainen tieto, kuten osoite tai puhelinnumero.
- Yksinkertainen numero- tai kirjainsarja.
- Jokin edellä mainituista takaperin.
- Jokin edellä mainituista sanoista jatkettuna numerolla.
- Urheilujoukkueet tai kuuluisan ihmiset.

Vahvoilla salasanoilla on seuraavia piirteitä:

- Ne sisältävät sekä isoja että pieniä kirjaimia.
- Niissä on numeroita ja välimerkkejä (esimerkiksi 0-9, !”#¤%&/()=?@${[]+-~:;,.\).
- Niissä on vähintään kahdeksan alfanumeerista merkkiä.
- Eivät ole minkään kielen, slangin, murteen tai vastaavan sanoja.
- Eivät perustu henkilökohtaisiin tietoihin, kuten perheenjäsenten nimiin tai vastaaviin.

(Thomas 2004, 161.)

3 Yritys

Suomesta löytyy tuhansia yksityisyrittäjiä, jotka työllistävät taas tuhansia muita ihmisiä. Kaikki näistä yrityksistä eivät välttämättä suoraan työllistä ihmisiä, mutta ne työllistävät väkeä omilla tarpeillaan sekä toimillaan. Heillä voi olla yrityksissään tärkeitä tietoja, jotka vaikuttavat muihin yrityksiin, ihmisiin, yhdistyksiin jne. On siis tärkeää, että yritykset edes hieman perehtyvät nykyiseen tietotekniikkaan, jos niissä sitä käytetään.

Otetaan esimerkki henkilöstä, joka on yksityisyrittäjä ja pyörittää tilitoimistoa. Hänellä voi olla tietokoneella monien yritysten tilinpäätökset. Kriittisellä hetkellä tietokoneen kaatuminen ja tiedostojen tuhoutuminen voi aiheuttaa suuria vahinkoja. Tämän takia yritysten tulee tietää keinoja turvata liiketoiminta, sekä varautua tuleviin mahdollisiin uhkiin.

On hyvä myös muistaa, että reilusti yli puolet tietoturvallisuuden ongelmista tietojärjestelmissä johtuu ihmisen toiminnasta, vain pieni osa laitteista, olosuhteista ja ohjelmistoista. Kun tilanne on tämä, ei pienenkään yrityksen tietoturvallisuutta voida hoitaa yksinomaan tietoteknisin ratkaisuin. Tarvitaan yleisiä periaatteita ja ohjeita tietoturvallisuudesta yrityksessä. (Teollisuuden Työnantajat 2001, 17.)

3.1 Riskien tuntemus

Suurimmat tietoturvallisuuden ongelmat liittyvät huolimattomuuteen, ymmärtämättömyyteen, osaamattomuuteen ja muihin tietojärjestelmien teknisen toteutuksen ja käytön laadullisiin tekijöihin. Panostaminen tietojärjestelmien käyttö- ja toimintaympäristössä työskenteleviin ihmisiin ja turvallisuustietoisuuden lisäämiseen, sekä yhteiskunnan tuki tehokkaalle ja turvalliselle tietojenkäsittelylle menevät aina yksinomaisten tietoteknisten ratkaisujen edelle tietoturvallisuuden rakentamisessa. Tietotekniikan merkitys on kuitenkin korostunut ja tulee korostumaan entisestään tietojärjestelmien ja rakenteiden monimutkaistuessa. Tämä taas on suuri ongelma tiedon käytettävyyden ja saatavuuden näkökulmasta. (Teollisuuden Työnantajat 2001, 10.)

Informaatioteknologian sovellukset sekä tietoverkkojen hallinta ovat monimutkaistuneet ja vaikeutuneet. Yhä harvemmat hallitsevat niiden toimintaa ja tietoverkkojen turvallisuutta. Sen vuoksi tietoturvallisuutta ja erisyisesti tietojärjestelmiin tunkeutumiseen käytettyjä tekniikoita, menetelmiä ja niiden vastatoimia hallitsevien henkilöiden palkkaaminen on selvästi lisääntynyt niin kansainväli-

sesti kuin Suomessakin. Myös tietojärjestelmään tunkeutumisen ilmaisevia ohjelmia (IDS, Intrusion Detection System) on tuotu markkinoille ja niitä on alettu hankkia (esimerkiksi RealSecure, NetRanger) (Teollisuuden Työnantajat 2001, 10.)

Yrityksen tietoturvallisuuden lähtökohtana tulee olla sen tosiasian tunnustaminen, että jokaisen yrityksen tiedot voivat olla väärinkäytösten kohteena. Tämän todellisuuden vähätteleminen voi olla koko yritystoiminnan kannalta kohtalokasta. Tietoturvatoimenpiteiden tarkoituksena on varmistaa yritystoiminnan kannalta tärkeiden tietojen hallinta sovittavien pelisääntöjen mukaisesti. Pelisäännöt tarkoittavat yritysjohdon kannanottoa siihen, miten asiat järjestetään niin, että asiattomat ja ulkopuoliset eivät saa kontrolloimattomasti haltuunsa yrityksen tärkeitä tietoja. (Teollisuuden Työnantajat 2001, 11.)

Kannattaa muistaa myös, että pitää varautua suojautumaan erilaisten vikojen, luonnontapahtumien tai tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta (tulipalot, vesivahingot, varkaus, ilkivalta, ukkosmyrsky, vahingot, laiteviat jne.).

Koska tietoturvallisuus riippuu yrityksen jokaisen henkilön toiminnasta, on tärkeää, että yrityksellä on tietoturvallisuuden keskeisiä asioita koskeva ohjelma. Ohjelmasta käyvät selkeästi ilmi vastuut, yleiset periaatteet, yrityksen tietoturvallisuusohjeistus, perehdyttäminen, koulutus, ylläpito ja kehittäminen sekä toimintaohjeet ongelma- ja väärinkäyttötapausten varalta. (Teollisuuden Työnantajat 2001, 12.)

3.1.1 Riskianalyysi

Riskianalyysin tarkoituksena on analysoida, arvioida ja kerätä tietoa siitä, mitkä asiat voivat aiheuttaa yrityksen toiminnan lamaantumisen tai vakavasti rajoittaa sen toimintaa. Esimerkiksi Internetistä löytyy useita valmiita ohjeita riskianalyysin toteuttamiseksi.

Riskianalyysi sisältää tarvittavan yksityiskohtaisen tiedon kaikista organisaation tiedoista, joihin kohdistuu sellaisia uhkia, joihin on syytä varautua tai joilta pitää suojautua. Riskien seurauksista – tietoturvaloukkausten seurauksista – laaditaan vaikutuskartoitus (impact analysis), joka kertoo toteutuneiden riskien vaikutuksen organisaation toimintaan ja tietoturvaan. (Tammisalo 2007, 31.)

Arvioi, mitä taloudellisia, teknisiä, juridisia ja toiminnallisia vahinkoja tietoturvaonnettomuus aiheuttaisi. Riskianalyysin on sisällettävä asiakkaille ja yritykselle aiheutuvat mahdolliset vahingot.

Analysoi lisäksi yksilölliset tietoturvauhat ja se miten ne vahingoittaisivat eri osastoja. (Myhr ym. 2004, 35.)

3.1.2 Verkkojen tietoturvaorganisaatiot

On hyvä tietää, mistä saa kerättyä tietoturva-asioihin asianmukaista ja ajankohtaista tietoa. En kerro perusteellisemmin kyseisistä organisaatioista, mutta kannattaa käydä tutustumassa sivustoihin, joita löytyy alla olevasta listasta. Nämä organisaatiot keräävät tietoja nykyisin tunnetuista haavoittuvuuksista ja niistä voi hakea lisää tietoa koskien tietoturvaa:

- http://www.cve.mitre.org/ (sanakirja)
- http://www.cert.org tai http://www.cert.fi
- http://www.sans.org
- http://www.cisecurity.com
- http://www.sans.org./score
- http://www.isc.sans.org
- http://nvd.nist.gov/
- http://www.securityfocus.com

CVE (common vulnerabilities and exposures)on luettelo standardoiduista haavoittuvuuksien nimistä ja muista tietoturva-altistuksista.

CERT (Computer Emergency Response Team) on Internet-tietoturvan asiantuntijakeskus. Se käsittelee tietokoneiden turvallisuuteen liittyviä tapahtumia ja haavoittuvuuksia sekä julkistaa tietoturvahälytyksiä, tutkii verkkojärjestelmien pitkäaikavälin muutoksia jne.

SANS (SysAdmin, Audit, Network, Security) on laajalti tunnustettu johtava organisaatio tietoturvan tutkimuksessa, sertifioinnissa ja koulutuksessa.

CIS (Center of Internet Security) määrittelee tehtäväkseen auttaa organisaatioita kautta maailman hallitsemaan tehokkaasti tietoturvaan liittyviä riskejä.

Score on SANS/GIAC:n ja Center of Internet Securityn (CIS) yhteistyöhanke. Se koostuu eri organisaatioiden tietoturva-ammattilaisista, jotka työskentelevät kehittääkseen yhteiset minimistandardit sekä parhaita käytäntöjä koskevan tietovarannon.

Internet Storm Center (ISC) on keskus, joka kerää päivittäin yli kolme miljoonaa tunkeutumisen havaitsemisen lokikirjausta.

NVD (National Vulnerability Database) on tietokoneiden haavoittuvuuksia sisältä hakutietokanta.

Security Focus on maailman laajin tietoturva-ammattilaisten yhteisö.

(Thomas 2004, 35.)

3.1.3 Tietoturvakäytännöt (tietoturvapolitiikka)

Jokaisella yrityksellä, joka käyttää tietojärjestelmiä, missä voi olla yritykselle tärkeitä tietoja, tulisi olla tietoturvakäytäntö. Tietoturvakäytäntöjen luominen on tärkeä askel verkon suojaamisessa ja turvaamisessa. Käytännöillä luodaan perussäännöt hyväksyttävälle ja sopivalle käyttäytymiselle yrityksessä ja verkossa. Käytännöistä tulee ”oikeusohje”, johon kaikkea muuta verrataan. (Thomas 2004, 47.)

Yrityksen tietoturvakäytäntöjä voidaan verrata yhteiskunnan sääntöihin ja lakeihin. Ilman niitä olisi mahdoton saada aikaan mitään arvokasta, ja tilanne voisi olla kaoottinen. Tieturvakäytäntö määrittelee, mikä on soveliasta sekä verkossa että sen ulkopuolella. Tämä on tietoturvakäytännön perustehtävä, mutta sen käyttökelpoisuudelle on olemassa monia muitakin perusteluja. Tietoturvakäytäntö:

- luo menettelytapoja koskevat odotukset
- määrittelee soveliaan käyttäytymisen
- kuvaa toiminnalliset ja liiketoiminnalliset periaatteet
- toimii väärinkäytöstapauksissa perustana henkilöstöhallinnon toimenpiteille
- määrittelee eri ryhmien roolit ja vastuut turvallisuuden takaamisessa
- toimii väärinkäytöstapauksissa tukena mahdollisille juridisille toimenpiteille
- määrittelee verkon tietoturvassa tarvittavat käsitteet ja mallit
- määrittelee mitä työkaluja tietoturva edellyttää ja toimii perusteena niiden hankintakustannuksille.

(Thomas 2004, 48.)

Tieturvakäytännön ansiosta yrityksen työntekijät ovat selvillä siitä, kuka on vastuussa mistäkin. Tietoturvakäytännössä määritellään yrityksen eri osastojen käytännöt ja prosessit. Näin esimerkiksi asiakaspalvelu tietää, että sen vastuulla on arkaluontoisten asiakastietojen suojaaminen, henkilöstöhallinto tietää, mitä työntekijöiltä tulee odottaa, ja valmistus ja tuotekehitys ymmärtävät, miten niiden

työn kallisarvoiset tulokset on suojattava. Tärkein tietoturvakäytännön tulos on tietenkin, mitä se tarkoittaa tietohallinnon kannalta. Tietohallinto osaa tällä perusteella konfiguroida palvelimet, tietää mitä työkaluja se tarvitsee ja osaa määritellä palomuurien säännöt, VPN-asetukset – luettelo on lähes loputon. (Thomas 2004, 48.)

Yrityksissä, joissa tietoturvallisuudella on strategista, toimintaan ja kilpailuun liittyvää merkitystä, olisi laadittava toiminnan perusteeksi tietoturvakäytäntö eli tietoturvapolitiikka. Muutoin kirjataan yleensä keskeiset periaatteet käytännön tietoturvallisuustyölle. Hyväksyessään nämä periaatteet yrityksen johto sitoutuu noudattamaan tietoturvapolitiikkaa ja velvoittaa henkilöstöä noudattamaan sitä. (Teollisuuden Työnantajat 2001, 17.)

PK yrityksen tietoturvapolitiikka (tietoturvakäytäntö) voisi olla seuraavan sisältöinen: Yrityksen liiketoiminnan ja taloudellisten etujen turvaamiseksi sekä erityisesti oikean, luotettavan tiedon saamiseksi ja tietojen käsittelyssä mahdollisesti aiheutuvien vahinkojen ennalta ehkäisemiseksi toteutetaan yrityksessä tietoturvallisuutta korostaen, että:

- Yrityksen tietoasiakirjat, tietovälineet, tekniset tallenteet ja suullinen informaatio ovat yrityksen omaisuutta ja niiden antaminen yrityksen ulkopuolelle saa tapahtua vain yhtiön eduksi.
- Yrityksellä on erilliset, kirjalliset ohjeet yrityssalaisen informaation merkitsemistä, käsittelyä, säilyttämistä ja hävittämistä varten.
- Esimies antaa ohjeet tiedoksi jokaiselle työntekijälle työsopimuksen solmimisen tai toimeksiannon yhteydessä.
- Jokainen työntekijä noudattaa tietoturvallisuudesta annettuja ohjeita ja vastaa omalta osaltaan tietoturvallisuudesta yrityksessä.

(Teollisuuden Työnantajat 2001, 17.)

Internetistä löytyy hyviä runkoja tietoturvakäytännöille, jos yrityksestä ei löydy ammattitaitoa sellaisen tekemiseen. SANS:n tietoturvakäytäntöjen projekti (http://www.sans.org/resources/policies) tarjoaa useita vaihtoehtoja tietoturvakäytännöiksi. (Thomas 2004, 48.) Edeltävän alaluvun (6.1.2) muillakin sivustoilla kannattaa käydä tutkimassa aiheeseen liittyvää materiaalia.

3.2 Tietoturvan laatu

Monissa yrityksissä alkaa nykyään olla käytössä laatustandardit tai vastaava laatuohjelma. Tarkoitus on, että yrityksen kannalta tär-

keimmät toiminnot ja prosessit ovat dokumentoidut ja jatkuvan kehityksen kohteena. (Teollisuuden Työnantajat 2001, 16.)

Yrityksen tietoturvallisuus on sellainen tärkeä alue eli laatutoiminnan moduuli, joka myös olisi toteutettavissa osana yrityksen muun toiminnan laatua (laatukäsikirjaa). Tietoturvallisuusasioiden tulisi olla osa päivittäistä toiminnan dokumentointia, ylläpitoa, koulutusta ja jatkuvaa parantamista. Kansainvälisiä tietoturvastandardeja on olemassa, kuten esimerkiksi BS 7799:1995, jota voi hyödyntää laatutyössä. Sellaisenaan se on melko raskas työväline otettavaksi käyttöön PK-ympäristössä. Standardi on käännetty suomeksi ja on saatavissa Suomen standardisoimisliitosta (BS 7799-1:fi,). (Teollisuuden Työnantajat 2001, 17.) Muita standardeja on ISO 17799, ISO 27000 – ISO 27005 ja sitten on vielä Infomation Security Forum:n (ISF) kehittämä standardi. ISF on kansainvälinen järjestö, jonka jäseninä on lähes 300 organisaatiota ympäri maailmaa. Suurin osa jäsenistä on suuria yrityksiä ja Suomesta jäseniä löytyy vajaat 15. Tärkein heidän tuotoksensa on ”Standard of Good Practise for Information Security” eli heidän oma standardinsa. (Laaksonen ym. 2006, 90.)

3.3 Laki tietoturvallisuudessa

Suomen lainsäädäntö on kansainvälisestikin arvioiden erittäin edistyksellinen tiedon salassapidon ja erityisesti yritysvakoilun, yritys-salaisuuden väärinkäytön osalta. Tietoturvallisuuteen liittyvää lainsäädäntöä on viime vuosina lisätty ja kehitetty edelleen. Vakoilusäädäntö, samoin kuin tieto- ja viestintärikosten kriminalisointi on varsin uutta. Atk ja tietotekniikka on otettu huomioon kohteena tai rangaistavan teon tekemisen välineenä useissa ns. tavallisissa rikoksissa. (Teollisuuden Työnantajat 2001, 14.)

Suomi on ollut esimerkillinen myös virusongelmien vastaisessa kansainvälisessä toiminnassa, kun se ensimmäisenä on kriminalisoinut tietokonevirusohjelman tekemisen ja levittämisen (RL 34:9a: Vaaran aiheuttaminen tietojenkäsittelylle). (Teollisuuden Työnantajat 2001, 14.)

Yritystä suojelevat Suomen laissa monet kohdat, mutta nämä asiat olisi hyvä tuoda henkilöstölle tiedoksi. Seuraavat lait ja sopimukset määrittelevät minkälaiset vastuut kohdistuvat työntekijöille: työsopimuslaki, yhteistoimintalaki, vilpillinen kilpailu (eli laki sopimattomasta menettelystä elinkeinotoiminnassa), rikoslaki, yrityssalaisuus, vaitiolo- ja salassapitosopimus.

3.4 Tietoturvallisuusohjelma

Yrityksen tietoturvallisuusohjelma perustuu tietoturvapolitiikkaan (tietoturvakäytäntö) ja yrityskohtaiseen tietoriskien analyysiin. Mitkä ovat meidän toimintamme kannalta kaikkein merkittävimmät tietoriskit ja miten ne hallitaan yrityksessämme? Mikä on yritysjohdon kannanotto ja sitoutuminen tietoturvallisuuden edistämiseen ja ylläpitämiseen yrityksessä eli tietoturvallisuuspolitiikka/tietoturvakäytäntö? Siinä on pari hyvää kysymystä esitettäväksi yritykselle. (Teollisuuden Työnantajat 2001, 18.)

Tietoturvallisuusohjelman ei tarvitse olla laaja. Sen keskeinen tavoite on antaa suuntaviivat ja sisältö yrityksen tietoturvallisuusmenettelylle ja -kulttuurille. Hyviä tietoturvallisuuden avainkohtia on:

- Sisällytä yrityksen hallituksen tai toimitusjohtajan kannanotto tietoturvallisuusohjelman johdanto-osaan. Tietoturvallisuuden ja yrityssalaisuuksien suojaamisen on lähdettävä yrityksen johdon tahdosta.
- Kuvaile ohjelman tarkoitus ja tärkeys. Henkilöstön on ymmärrettävä ja miellettävä keskeinen roolinsa ja vastuunsa tietoturvallisuuden toteuttamisessa.
- Erittele tarkoin, keitä kaikkia toimintaohjelma koskee. Muista omena henkilöstön osalta myös toisiin tehtäviin siirtyvät, eroavat ja erotetut henkilöt sekä laajasti kaikki ulkopuoliset sidosryhmät (ulkopuoliset palvelut, alihankkijat jne.).
- Tee yrityssalaisuuksien käsittelyn ja muun tietoturvallisuuden kannalta tärkeiden avainhenkilöiden kanssa salassapitosopimus, joka koskee yrityssalaisuuksien lisäksi mm. kilpailevaa toimintaa ja työsuhdekeksintöjä. Tämä on tärkeää tehdä myös ulkopuolisten alihankkijoiden ja järjestelmäntoimittajien kanssa sekä kaikkien niiden kanssa, joilta hankitaan palveluja. Muista, että yrityksesi on vastuussa myös asiakkaiden, laitteistotoimittajien ja muiden sidosryhmien tietojen turvallisuudesta.
- Määrittele, mikä tietoaineisto on suojatta. Ohjelmaan sisällytetään suojattavan tiedon yleiset ja erityiset periaatteet.
- Määrittele ja ohjeista tiedon luokitteluperiaatteet siten, että jokainen tuntee ja tietää menettelyn.
- Nimeä yhdyshenkilöt tärkeimpiin toimintayksikköihin tukemaan tietoturvallisuusmenettelyä ja vastuita. Tiedota nimetyt henkilöt yrityksen koko henkilöstölle.
- Määrittele toimenpiteet väärinkäytösten tai rikollisen toiminnan varalta. Kirjaa ne toimenpiteet, jotka ovat tärkeitä selvitettäessä, mitä ja milloin on tapahtunut. Nimeä henkilö, johon otetaan yhteyttä, kun jotain yrityksen tietoturvallisuuspelisääntöjen kannalta epäilyttävää on tapahtunut.

- Määrittele tiedon käsittelyn, säilyttämisen, välittämisen, kirjaamisen, kopioinnin sekä hävittämisen periaatteet ja menettelytavat.
- Järjestä tietoturvallisuuskoulutusta ja -valmennusta henkilökunnalle. Käytä tiedottamista ja julkaisuja hyväksesi pitääksesi yllä turvallisuustietoisuutta yrityksessäsi.
- Määrittele, kuka on vastuussa tietoturvallisuusohjelman toteuttamisesta.

(Teollisuuden Työnantajat 2001, 18.)

Tärkeitä periaatteita tietoturvallisuusohjelmaa rakennettaessa:

- NEED TO KNOW – kuka tietoa tarvitsee
- NEED TO HOLD – kuka tietoa säilyttää
- CLOSE TO YOU – tietoturvallisuusvälineet (kaapit, paperisilppurit, yms.) ovat lähellä sinua ja työskentelytiloissasi

Tietoa on paljon ja sitä on yrityksessä eri muodoissa. Hallittu tietojen käsittely edellyttää yhteisiä pelisääntöjä. Edellä kirjatut periaatteet tarkoittavat käytännössä mm. sitä, että kaikki tieto, joka on kunkin henkilön tehtävän kannalta tärkeää, on hänen saatava. Kaikkia tietoja ei jaeta kaikille. (Teollisuuden Työnantajat 2001, 19.)

Tietoturvallisuuden hoitamiseksi tarvittavat välineet on hankittava ja sijoitettava järkevästi: paperisilppuri kopiokoneen viereen tai läheisyyteen ja avainhenkilön työhuoneeseen. Muutoin niitä ei juuri käytetä. Sama koskee palo- ja murtoluokiteltua kassa- tai turvakaappia, jossa säilytetään tärkeimpiä asiakirjoja ja tietovälineiden varmuuskopioita. (Teollisuuden Työnantajat 2001, 19.)

3.5 Fyysinen ympäristö

Fyysisellä turvallisuudella taataan yritykselle häiriötön ja turvallinen toimintaympäristö. Jokainen organisaatio tarvitsee fyysiset tilat toimintansa harjoittamiseen. Toimitilojen suojaaminen luo perustan kaikille muille suojaustoimille, joita tietoturvallisuuden ylläpitämiseksi käytetään. Ilman turvallista toimintaympäristöä ei tiedon luotettavuutta voida aukottomasti varmistaa. Tietojen käsittelyn fyysisen turvallisuuden suunnitteluun tarvitaan usein koko toimintaympäristön kattava turvallisuustarpeiden ja -ratkaisujen arviointi. (Laaksonen ym. 2006, 125.)

Kaikki yrityksen tilat eivät ole fyysisen turvallisuuden kannalta samanarvoisia. Yleensä korkeaa suojausta vaativia kohteita ovat yrityksen omiin vahvuusalueisiin liittyvät tilat, esimerkiksi tuote-

kehitystilat, atk-laitetilat sekä hallinnolliset tilat. Ylipäätään fyysisen turvallisuuden suunnitelman piirissä tulisi olla kaikki tilat, joissa käsitellään yrityksen toiminnalle merkityksellistä tietoa. Fyysinen toimintaympäristö tulee arvioida säännöllisesti riskikartoitusten yhteydessä. Korjaus- ja kehitysehdotukset tulee kirjata ylös ja toteuttaa yleisen rakennus- ja korjaushankkeiden yhteydessä. (Laaksonen ym. 2006, 125.)

Fyysisen turvallisuuden asianmukainen järjestäminen on periaatteessa helppoa ja siihen on saatavissa lisäohjeita monilta tahoilta. Tietojenkäsittelytilojen suojaamiseen on laadittu useita erilaisia tarkistuslistoja. ISO 27001 -standardi sisältää omat vaatimuksensa, ja esimerkiksi Suomen puolustusvoimat määrittelee turvalliset tilat hyvinkin tarkasti. Samoin VAHTI-ohjeissa sekä Viestintäviraston ja Rahoitustarkastuksen dokumenteissa otetaan kantaa tilojen suojaukseen. (Laaksonen ym. 2006, 125.)

Fyysinen turvallisuus sisältää yrityksen tuotanto- ja toimitilojen fyysisen suojaamiseen liittyvät asiat, joilla pyritään estämään organisaation tarvitsemien tietojen tuhoutuminen, vahingoittuminen tai joutuminen vääriin käsiin. (Laaksonen ym. 2006, 126.)

Seuraavaksi on lueteltu tietotekniikkalaitteiden ja laitetilojen suojaukseen liittyvät asiat, joiden avulla estetään luvaton tietoihin pääsy sekä suojataan tietoja katoamiselta tai vahingoittumiselta. Toimitilat tulee suojata ainakin seuraavilta asioilta:

- varkaus (kiinteistön hälytysjärjestelmä, panssarilasit)
- tulipalo ja lämpötilan liiallinen kohoaminen (palovaroittimet, sammutusjärjestelmät, paloturvakaapit, ilmastointi)
- vesivahinko ja kosteus (nostaa laitteet pois lattiatasosta, laitetiloissa ei ole vesiputkia)
- sähköhäiriö (ylijännitesuojat, UPS-laitteet ja varageneraattori, laitteiden toimivuus tulee testata säännöllisesti)
- pöly (säännöllinen siivous, tilan käytön rajoittaminen)

(Laaksonen ym. 2006, 127.)

Kannattaa muistaa myös tarkistaa vakuutusyhtiön vaatimukset. Noudattamalla vakuutusyhtiöiden vakuutuskirjojen vaatimuksia monet tietoturvan kannalta oleelliset kohteet tulee suojattua. Vakuutuskirjan vaatimukset ovat hyvä lähtökohta organisaation jatkuvuussuunnitelmalle mahdollisten kriisien varalle.

3.6 Henkilöstö

Yrityksen jokaisen työntekijän tulee huolehtia omalta osaltaan tietoturvallisuuspolitiikan tavoitteiden saavuttamisesta. Jotta työntekijä voi toimia tavoitteiden mukaisesti, on hänen osallistuttava yrityksen tietoturvallisuuskoulutuksiin sekä aktiivisesti sovellettava tietoturvaohjeita ja -toimintatapoja käytännön työtehtäviin. (Laaksonen ym. 2006, 137.)

Jokainen työntekijä toimii työsopimuksensa ja muiden sopimusten sekä sitovien ohjeiden mukaisesti. Henkilöstön tulee suhtautua yrityksen tietoon ohjeiden mukaan ja noudattaa huolellisuutta tietojen käsittelyssä. Kriittisistä ja tärkeistä tehtävistä vastaava henkilö huolehtii siitä, että hänen varahenkilönsä tiedot ovat ajan tasalla.

Henkilöstön tehtäviä ovat:

- Tiedon luokittelu ja käsittely ohjeiden mukaisesti.
- Luokitellun tiedon käsittely, siirtäminen ja säilyttäminen ohjeiden mukaisesti.
- Omien salasanojen hallinta ja turvallinen käyttö.
- Ohjeiden noudattaminen.
- Varahenkilön tiedottaminen ja koulutus.
- Heikkouksien ja puutteiden raportointi sovittuja raportointikanavia käyttäen.

(Laaksonen ym. 2006, 137.)

Palkattaville henkilöille voi tarvittaessa tehdä turvallisuusselvityksen esimerkiksi silloin, kun yritykseen palkataan uusia henkilöitä avaintehtäviin tai tehtäviin, joissa he joutuvat käsittelemään yritys-salaisia tietoja. Luotettavuustarkistus voi koskea myös yrityksen sidosryhmiä ja niiden edustajia, kuten ulkopuolisia palveluja, alihankkijoita, tai esimerkiksi ulkomaalaisia henkilöitä, jotka tulevat yritykseen neuvottelemaan ja yhteisiin projekteihin. Turvallisuusselvitykset ovat suojelupoliisin lakisääteistä toimintaa. Selvitystä voidaan pyytää suojelupoliisilta lähinnä silloin, kun on kyseessä valtakunnan turvallisuus tai merkittävät taloudelliset edut. (Teollisuuden Työnantajat 2001, 21.)

Henkilöstöä koskee tietenkin Suomen laissa määritetyt säädännöt vaitiolosta ja salassapidosta (lain 6. luvussa salassapitovelvoitteet, 24§:n 32 erillistä kohtaa) (Teollisuuden Työnantajat 2001, 22). Kannattaa siis muistaa, että vaitiolo koskee automaattisesti kaikkia. Kannattaa kuitenkin varmistaa yrityksen salaisten tietojen turvallisuus erillisillä salassapito- ja vaitiolosopimuksilla.

3.6.1 Henkilökunnan koulutus

Monet tietoturvaperiaatteet kariutuvat laiskuuden, osaamattomuuden tai muiden inhimillisten tekijöiden vuoksi. Vaikka tietoturvaperiaatteet olisi muotoiltu miten hyvin ja laajasti tahansa, ne toimivat käytännössä vain, jos ne tunnetaan ja niistä vastuussa olevat henkilöt voivat noudattaa niitä.

Koulutus kannattaa jakaa yleiseen osaan, jossa käsitellään kaikkia koskevia aiheita, sekä osaan, jossa henkilöstöä opetetaan käyttämän tietoturvan apuvälineitä. Tämä edellyttää erityistä sitoutumista hallinnollisilta vastuuhenkilöiltä, jotka esimerkiksi vastaavat käyttöoikeuksista, palomuurin toiminasta ja varmuuskopioinnista. (Myhr ym. 2004, 37.)

Koulutuksen järjestäminen sisäisenä seminaarina tai luokkahuoneopetuksena painottaa tietoturvakysymysten tärkeyttä. Tämä auttaa ymmärtämään tietoturvan merkityksen ja vahvistamaan henkilöstön sitoutumista. (Myhr ym. 2004, 37.)

Koulutus kannattaa jaksottaa pitkälle aikavälille. Tämä osoittaa, että yrityksen tietoturvatyö on pitkäjänteistä ja että näitä oppeja ei ole tarkoitus unohtaa viikossa eikä vuodessa. Yrityksen järjestelmissä ja toiminnassa tapahtuvat muutokset ja uusi henkilöstö voivat olla syy koulutuksen uusimiseen. (Myhr ym. 2004, 37.)

Tässä lyhyt lista henkilökunnan kouluttamisesta:

- Muista selvittää toimintatapojen lisäksi syyt. Käyttäjät omaksuvat tiedot helpommin, jos heille selvitetään ongelma ja sen ratkaisu.
- Toista koulutus usein. Kerro tärkeistä asioista ja perustele, miksi ne ovat tärkeitä.
- Laadi tietoturvatoimintaperiaatteista tarkistusluettelo ja aseta se näkyville paikoille, kuten kahvihuoneeseen jne.
- Anna henkilöstölle muistilappu tai pöytäkortti, jota he voivat pitää työpöydällä.
- Varmista, että tietotekniikkaa koskevat tietoturvatoimintaperiaatteet ovat kaikkien tiedossa.

(Myhr ym. 2004, 37.)

3.6.2 Etätyö

Tietokoneen avulla tehtävä etätyö on yleistynyt. Jatkuvasti paranevat tietoliikenneyhteydet vauhdittavat tätä kehitystä. Koska etätyö edellyttää usein sisäisten järjestelmien avaamista ulkoiselle tietolii-

kenteelle, monia tärkeitä tietoturvanäkökohtia on tarkasteltava perusteellisesti. (Myhr ym. 2004, 15.)

Yleisesti ottaen etätyöpisteessä on vaikea valvoa tietoturvallisuutta yhtä tehokkaasti kuin toimistossa. Siksi kannattaa mieluummin vähentää etätyön tietoturvariskejä ja niiden mahdollisia seurauksia, kuin pyrkiä samaan tietoturvan tasoon kuin toimistossa. Ennen kaikkea on pyrittävä mahdollisuuksien mukaan välttämään tärkeiden tietojen tallentamista kannettavaan tai kotitietokoneeseen. (Myhr ym. 2004, 15.)

Etätyön yleiset varo-ohjeet:

- Käsittele luottamuksellista aineistoa huolellisesti.
- Älä anna muiden ihmisten tai perheenjäsenten käyttää työskentelyyn tarkoitettua tietokonettasi.
- Älä koskaan jätä tietokonetta ilman valvontaa tai lukitsematta. Varmista, että salasanalla varustettu näytönsäästäjä suojaa tietokonetta, kun et käytä sitä.
- Ole erityisen huolellinen lentokentillä tai hotelleissa. Pidä tietokone aina käden ulottuvilla ja lukittuna kantolaukkuunsa.
- Jos tietokone varastetaan, ilmoita asiasta heti tietotekniikkavastuuhenkilölle ja esimiehellesi.
- Jos lataat ohjelmia tai tiedostoja Internetistä, tutki ne ennen asentamista.
- Älä asenna ohjelmistoa, johon ei ole käyttöoikeuksia. Tarkista ennen asentamista, että yritys on hyväksynyt ohjelman asentamisen.
- Yrityksen tietoja saa käyttää vain työntekoon tarkoitetulla tietokoneella.
- Yrityksen verkkoon saa muodostaa vain VPN-yhteyden.
- Tietokone on suojattava sekä virustorjuntaohjelman että työasemakohtaisen palomuurin avulla.

(Myhr ym. 2004, 16.)

3.6.3 Työ- ja liikematkat

Jokainen on matkoilla yrityksensä edustaja ja avainhenkilö. Paikoissa, joissa sivulliset voivat kuulla (julkiset kulkuvälineet, ravintolat jne.), tulee välttää keskustelua yrityssalaisuuksista. Sama tilanne voi koskea myös tuttavia, kaveripiiriä ja sukulaisia. Mukana pidetään vain tarpeelliset asiakirjat ja tietovälineet, joita tarvitaan työskenneltäessä esimerkiksi kannettavalla tietokoneella. Yrityssalaisia tietoja ei taltioida kiintolevylle, vaan muille sopiville tietovä-

lineille (disketti, CD-rom, DVD ja muistitikku), ellei käytössä ole erityinen salakirjoitusohjelma. Salakirjoitusta kannattaa käyttää myös tärkeiden tietojen kohdalla muissakin tietovälineissä. Jos kannettava tietokone anastetaan, ei samalla menetetä tärkeitä tietoja. (Teollisuuden Työnantajat 2001, 24.)

Matkapuhelinviestinnässä on otettava huomioon, että gsm-salaus on verkon ominaisuus, ei käyttölaitteen (ainakaan toistaiseksi). On tiedettävä, onko ao. maan gsm-operaattorilla verkossa salaus ja minkä tasoinen se on. (Teollisuuden Työnantajat 2001, 24.)

Matkapuhelimesta on myös syytä huolehtia. Sekin voidaan anastaa ja kustannusten lisäksi voidaan menettää tärkeitä tietoja, joita on välitetty esim. boxiin eli matkapuhelimen postilaatikkoon. Auki oleva matkapuhelin voi välittää neuvottelusta tai keskustelutilanteesta puheenvuorot sellaisenaan mihin tahansa paikkaan, jonne on soitettu ennen tilaisuutta ja jätetty matkapuhelin tarkoituksellisesti auki. Matkapuhelinta voidaan myös käyttää salakuunteluun omistajan tietämättä, niin kauan kuin siinä on akku kiinni. Nykyajan älypuhelimiin voi myös tarttua viruksia ja siksi nekin tulisi suojata torjuntaohjelmilla. (Teollisuuden Työnantajat 2001, 24.)

3.7 Kulunvalvonta

PK-yrityksissä yrityssalaisuuksia voi suojata tehokkaasti myös kulunvalvonnan ja vierailumenettelyn keinoin. Kulunvalvonta on olennainen osa työympäristön ja asioinnin turvallisuutta.

Kulunvalvonnan tarkoitus on pääsääntöisesti estää asiattomien tahojen pääsy yrityksen tiloihin ja sallia omien työntekijöiden kulku siellä, missä se on heidän työtehtäviensä kannalta tarpeellista. Kulunvalvonta on lain mukaan ”lievempi” vaihtoehto kuin kameravalvonta, ja työnantajan pitäisikin harkita ensin sen käyttöä ennen kuin turvaudutaan kameravalvontaan. Kulunvalvonnalla on myös mahdollisuus parantaa asiakaspalvelua, koska isommissa yrityksissä yleiset ”aulavahdit” voivat ilmoittaa asiakkaille, missä heidän etsimänsä henkilö kulloinkin on. (Laaksonen ym. 2006, 51.)

Kulunvalvonta voidaan hoitaa:

- Teknisellä valvonnalla, johon kuuluvat valvontakamerat ja erilaiset hälytyslaitteet, rikosilmaisimet.
- Henkilövalvonnalla (vartiointi, henkilöstön oma huomiointi).
- Kuten nykyisin useimmiten toteutetaan, näiden yhdistelmänä, jossa teknisen järjestelmän ilmoituksia ja kuvaa seuraa koulutettu valvontahenkilö(stö).

(Teollisuuden Työnantajat 2001, 23.)

Jokainen yrityksen henkilö voi osallistua kulunvalvontaan mm. siten, että ohjaa ystävällisesti mutta päättäväisesti asiattomat henkilöt oikeaan paikkaan. Työpaikalla ei ulkopuolisten henkilöiden tulisi voida kulkea ilman isäntää. Erityisesti on tärkeä muistaa, että jokainen vastaa omista vieraistaan ja heidän kulkemisistaan yrityksessä, joko omakohtaisesti tai sihteerin tai muun henkilön avustuksella. (Teollisuuden Työnantajat 2001, 23.)

Yrityksessä järjestettävät vierailut ja kokoukset tulee suunnitella etukäteen ja niin hyvin kuin mahdollista. Esimerkiksi kokoustilat ja kulkureitit on valittava huolella. Tulee välttää näyttämästä vieraalle sellaisia tietoja ja olosuhteita, joiden näyttäminen saattaa aiheuttaa yritykselle vahinkoa. (Teollisuuden Työnantajat 2001, 23.) Tarvittaessa ilmoitetaan ennakkoon kuvaus-, nahoitus- tai matkapuhelimen käyttökiellosta vierailun tai kokouksen aikana.

3.8 Yrityksen tarpeet

Yrityksen tietojärjestelmää toteuttaessa kannattaa huomioida mahdollinen yrityksen kasvu sekä kehittyminen. Hyvä tapa on kirjata paperille, millaisia tarpeita yrityksellä on koskien tietojärjestelmää. Esimerkiksi muutaman hengen yrityksen ei välttämättä kannata hankkia omaa sähköpostipalvelinta tai palvelinta Internet-sivustoille. Operaattoreilta ja ASP-yrityksiltä (Application Service Provider) saa ostettua kyseiset palvelut ja näin säästää rahaa ja vaivaa.

Tietotekniikkaan saa nopeasti investoitua suuri summia, joten on erittäin tärkeää tietää omat tarpeensa tietojärjestelmää koskien. Kannattaa vaikka konsultoida kyseistä yritystä, jolta ostaa laitteet, sekä konsultoida riippumatonta tahoa. Sama koskee myös ohjelmistoja, jotka parantavat tietoturvaa. Monia erittäin toimivia ohjelmistoja saa ilmaiseksi Internetistä, kannattaa vaan varmistaa, että voittoa tekevä taho eli yritys saa niitä käyttää.

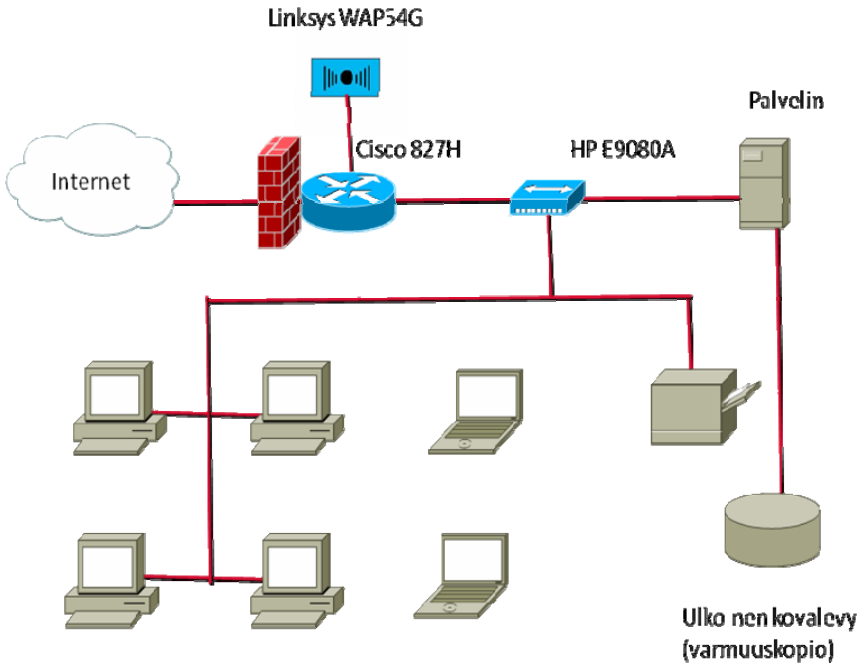
4 Käytännön esimerkki

Kerron seuraavaksi käytännön esimerkin pienyrityksen verkon toteuttamisesta, mikä helpottaa ymmärtämään edellä esiteltyjä asioita käytännössä. Esimerkissä on selvitetty kuinka toteuttaa teknisesti pienen yrityksen lähiverkko.

4.1 Lähiverkon rakenne

Yrityksen verkko käsittää reitittimen, jossa on kytkin, modeemi ja palomuuri samassa, langattoman tukiaseman, neljä pöytätietokonetta, monitoimisen tulostimen (laitteessa on kopiokone, tulostin, skanneri ja faksi), tiedostopalvelimen, kaksi kannettavaa tietokonetta, kytkimen ja ulkoisen kovalevyn.

Reitittimenä toimii Cisco 827H, joka on tarkoitettu ADSL-linjaan. Langattomana tukiasemana toimii Linksys WAP54G Wireless Access Point. Kytkimenä toimii HP E9080A (22 porttia). Tiedostopalvelimen käyttöjärjestelmänä on Windows Small Business Server 2003 R2.



Kuva 2. Lähiverkon rakenne

4.1.1 Reititin

Reitittimen asetuksista ensimmäiseksi muutettiin salasana. Tämän jälkeen voidaan aloittaa konfiguroimaan muita asetuksia. IP-osoitteiden jakaminen tiputettiin heti kymmeneen osoitteeseen, koska laitteen ei tarvitse useampia jakaa, IP avaruus on 10.10.100.10 – 20. Muutama osoite otettiin varalle. Reitittimellä on kiinteä IP-osoite 85.165.75.132.

Useimmissa laitteissa on nykyään oletuksena NAT (Network Address Translation) päällä, samoin myös tässä laitteessa. NAT piilottaa lähiverkon IP-osoitteet ulkopuolisilta yhden osoitteen taakse. Kyseinen ominaisuus pidettiin käytössä.

Reitittimellä on annettu kaikkien käytössä olevien laitteiden MAC-osoitteet ja kaikki muut ovat suljettu ulkopuolelle. Reititintä ei pääse konfiguroimaan kuin yhdestä portista ja yhdestä IP-osoitteesta. Kaikille muille koneille on laitettu kiinteät IP-osoitteet, paitsi kannettaville jaetaan osoitteet DHCP:llä (Dynamic Host Configuration Protocol).

Reititin sisältää myös palomuurin, jonka perusasetukset olivat tarpeeksi kattavat eli niihin ei tarvinnut koskea. Portteja avataan tarpeen mukaan. Seuraavat portit on avattu:

- 20, 21, tiedostojen kopiointiin käyttettävä protokolla (FTP, File transfer protocol)
- 22, salattujen etäyhteyksien muodostaminen (SSH, Secure Shell)
- 23, pääteyhteys (Telnet)
- 25, sähköpostin lähettäminen ja vastaanottaminen (SMTP, Simple Mail Transfer Protocol)
- 53, nimiselvitys (DNS, Domain Name System)
- 80, web-selaus (HTTP, Hypertext Transfer Protocol)
- 111, etäproseduurikutsut (RPC, Remote Procedure Call)
- 193, keskustelu (chat), (IRC, Internet Relay Chat)
- 443, salattu yhteys www-selailuun (mm. pankkiyhteydet ja verkkokauppa), (HTTPS, Hypertext Transfer Protocol Secure)

Reititin pitää myös sisällään VPN-tuen.

4.1.2 WLAN tukiasema

Langattoman tukiaseman SSID on ensimmäiseksi vaihdettu salasanamaiseksi (katso luku 2.14, s.30) ja otettu yleislähetys pois päältä. IP-tukiasemalla on kiinteä IP-osoite ja laitteen konfiguroin-

tiin tarvitaan käyttäjätunnus ja salasana. Laitteen konfigurointi tapahtuu web-liittymän kautta. Langattoman verkon asetuksissa on käytössä WPA(TKIP)-salaus (ks. s.20) (128-bittiä), jolla kryptataan kannettavien tietokoneiden ja langattoman tukiaseman välinen liikenne. Yleislähetysavainta vaihdetaan 10 minuutin välein. Tukiasemaan on asetettu MAC-suodatus johon on annettu kahden kannettavan MAC-osoitteet, muut suljetaan ulkopuolelle.

SSID ja WPA-avain vaihdetaan vuosineljänneksittäin, lähetys kanavaksi asetetaan kanava 13, sitä vaihdetaan tarvittaessa. Kannettavissa ei kannata pitää langatonta lähetintä päällä, jos niitä ei käytetä. Sama koskee myös bluetooth-lähetintä. Tämä siksi, että ne eivät altistaisi konetta tietoturvauhille ja kuluttaisi tietokoneen akkua.

4.1.3 Palvelin

Käyttöjärjestelmäksi on valittu Windows Small Business Server 2003, josta on otettu käyttöön AD (Active Directory), tiedostopalvelin, Windows backup ja shadow copy. Windows Small Business Server sisältää ohjatun varmuuskopio määrityksen, tämän avulla voidaan määritellä varmennettavat tiedostot, varmuuskopion tallennuspaikan (kiintolevy, nauha-asema jne.) ja kuinka usein varmuuskopiointi suoritetaan. Varmuuskopioinnin voi käynnistää myös manuaalisesti työkalun avulla. (Microsoft Corporation 2007.) Shadow copy toimii myös Windows XP professinal:ssa. Shadow copy pystyy ottamaan käynnissä olevista tiedostoista varmuuskopioita tai taltioita (niin sanottuja snap-shotteja). Toiminto toimii myös, jos varmuuskopiota tehdessä on joku tiedosto työn alla. Joskus olet voinut huomata, esimerkiksi Word:n kaatuessa, että Windows kysyy palautetaanko aikaisempi istunto. (Microsoft Corporation 2007.)

AD:hen tehtiin kaksi GPO:a (Group Policy), toinen käyttäjille ja toinen tietokoneille. GPO:ssa määriteltiin muun muassa salasanakäytännöt. Salasanakäytännöissä määritellään salasanan pituus, vanhetumis aika, virheellisten syöttöjen määrä, sekä salasanan kompleksisuus. AD otettiin käyttöön, koska yrityksen odotetaan kasvavan lähitulevaisuudessa. Tällä hetkellä ei ole vielä tarvinnut tehdä monimutkaisempia määrittelyjä.

Tiedostopalvelimella jaetaan käyttäjille yhteistä kovalevytilaa, sekä omat kansiot. Kaikki tärkeä informaatio tullaan tallentamaan ja pitää tallentaa palvelimelle. Johtohenkilöiden kansiot ovat suojattu muilta käyttäjiltä. Palvelimelta kaikki tiedostot saadaan varmuuskopioitua DVD-levyille, sekä ulkoiselle kovalevylle. Ulkoinen kovalevy laitetaan aina yöksi paloturvakaappiin. Palvelimessa on kaksi kovalevyä, jotka ovat peilattu keskenään.

4.1.4 Tietokoneet

Kaikissa tietokoneissa on Windows XP Pro SP2 -käyttöjärjestelmä. Tietokoneissa tietoturvaa kohennettiin ottamalla käyttöön näytönsäästäjään kytketty salasana, joka lukitsee koneen kymmenen minuutin viiveellä. GPO:ssa on myös määritelty, että jos konetta ei käytetä kymmeneen minuuttiin, koneet lukittuvat.

Kannettavissa tietokoneissa on otettu käyttöön BIOS-salasana, kiintolevyn salasana ja käyttäjätilin salasana. Tärkeimmät tiedot sisältävät kansiot kryptataan varmuuden vuoksi. Käyttäjiä on opastettu pitämään kannettavissa aina langaton radio sekä bluetooth pois päältä, kun niitä ei käytetä. Kannettavissa on myös erikseen asennettuna ohjelmistopalomuurit virustorjunnan lisäksi. Kaikissa tietokoneissa on virustorjuntaohjelmien lisäksi anti-spyware ohjelmisto, Windows Defender, sekä McAfee spyware asetukset päällä.

Virustorjunta ohjelmistona käytetään McAfee VirusScan Enterprise 8.5:tä. Virustutkasta on otettu päälle ei toivottujen ohjelmien (unwanted programs) asetus, jolla estetään spyware, adware, jokes, key-loggers ja dialers (haitta- ja vakoiluohjelmat).

Yleisenä käytäntönä kaikkia käyttäjiä on opastettu aina lukitsemaan tietokone (Ctrl-Alt-Del). Kannettavia tietokoneita ei koskaan saa jättää yleisiin tiloihin vartioimatta tai esimerkiksi autoon. Tietokoneet sisältävät arkaluontoista materiaalia ja niitä on käsiteltävä erityisellä huolellisuudella. Kannettavia tietokoneita ei myöskään saa antaa muiden henkilöiden käytettäväksi esimerkiksi kotona (koneet ovat henkilökohtaisia). Kannettavissa tietokoneissa on sormejälkitunnistus.

Käyttöoikeuksia on rajoitettu kaikissa tietokoneissa käyttäjän tarpeiden mukaan. Hallinto-oikeudet on annettu järjestelmänvalvojalle ja hänen varamiehelleen.

4.3 Varmuuskopiointi

Varmuuskopiointi suoritetaan päivittäin palvelimelta ulkoiselle kovalevylle. Varmuuskopiointi ajetaan Windows backup:lla. Joka maanantai tarkistetaan onko varmuuskopiointi suoritettu. Aikaisemmin mainittiin jo, että palvelimella on kaksi kovalevyä, jotka peilataan keskenään.

Varmuuskopiota säilytetään paloturvakaapissa, joka kestää myös perinteiset ryöstöyritykset. Ulkoinen kovalevy laitetaan joka päivä kaappiin. Kaappi on sijoitettu yrityksessä sellaiseen paikkaan, missä se ei ole ulkopuolisten nähtävillä, sekä on otettu huomioon kiinteistön osalta rakenteet koskien paloturvallisuutta ja vesivahinkoja. Palvelinkaappi on sijoitettu samaan tilaan.

5 Yhteenveto

Tietoturva on käsitteenä erittäin laaja, se ei pelkästään käsitä tietojärjestelmiä, vaan kaiken toiminnan mikä liittyy yrityksen toiminnan jatkuvuuteen. Tietoyhteiskunnan kasvaessa ja maailman kehittyessä tietoturva tulee monimutkaistumaan, minkä vuoksi tietoturvan tarve tulee myös kasvamaan.

Tietoturva on hyvä aloittaa pienessä yrityksessä teknisestä tietojärjestelmän toteutuksesta. Tarkoitus on varmistaa, että yrityksen tietojärjestelmä käsittää kaikki tarvittavat laitteet, jotka varmistavat tietojen säilymisen ja liiketoiminnan jatkuvuuden. Kun yrityksen tietoverkko laitteineen ja ohjelmistoineen on toiminnassa ja tietoturva on teknisesti varmistettu, on aika miettiä tietoturvakäytäntöjä.

Kannattaa muistaa, että ihminen on suurin tietoturvaongelmien aiheuttaja, joten on erittäin tärkeää, että yrityksen koko henkilöstö koulutetaan toimimaan tietoturvallisesti. Lehdistä voi lukea viikoittain, kuinka eri yritykset ovat joutuneet erilaisiin vaikeuksiin viruksien tai muiden uhkien takia. Kaikkien olisi syytä varautua selviytymään mahdollisista ongelmista, jopa kotitietokoneen käyttäjien. Digiaikana olisi ikävää, jos kaikki kuvat ja tärkeät tiedot katoaisivat koneelta ja ei olisi minkäänlaista varmuuskopiota.

Tietoturvasta huolehtiminen on kaikista tärkein tietojärjestelmiin liittyvä asia. Ilman riittävää tietoturvaa organisaatiot tai kotikäyttäjät eivät voi toimia vakaasti ja luotettavasti. Tietoturvan toteuttaminen ja sen ymmärtäminen on monimutkaista, mutta pakollista nykyisessä maailmassa.

5.1 Työn rajaus ja siihen liittyneet ongelmat

Saadessani idean tehdä tutkintotyön pienyritysten tietoturvasta en käsittänyt, kuinka laaja aihepiiri on. Haastavinta aiheen rajauksessa olikin päättää, mitkä olisivat oleellisia asioita liittyen PK-yrittäjän tietoturvaan. Tavoitteena oli selvittää ja esitellä pääpiirteittäin tärkeimmät tietoturvallisuuteen liittyvät asiat siten, että lukija saisi kokonaiskuvan tietoturvallisuuden tärkeydestä ja vinkkejä sen toteuttamiseen.

Aiheen käsitteleminen ja työn kirjoittaminen oli minulle erittäin haastavaa. Toivottavasti työstä olisi jonkinlaista hyötyä pienten yritysten omistajille ja työntekijöille yrityksen tietoturvan toteuttamisessa. Loppujen lopuksi olen itse tyytyväinen työhön, koska se ainakin herättää ymmärryksen tietoturvan tärkeyteen.

5.2 Loppusanat

Käsittelemäni aihe kiinnostaa itseäni edelleen ja siksi olen myös näin jälkeenpäin tyytyväinen valintaani. Sain idean aiheeseen jo yli vuosi sitten. Selailin silloin aiemmin tehtyjä tutkintotöitä ja kyseisestä aiheesta ei ollut tehty kovin montaa työtä. Tällä hetkellä, kun olen saanut työni valmiiksi, aiheesta on kuitenkin tullut muitakin töitä. Olisi siis pitänyt kirjoittaa nopeammin työ valmiiksi.

Työtä kirjoittaessani huomasin, kuinka vähän itsekään tiedän tietoturvallisuudesta. Tietoturvallisuus pitää sisällään lukemattomia asioita: kaiken mahdollisen tietojärjestelmiin, Internetiin ja verkkoihin liittyvän. Aiheesta löytyy tietoa ja tutkimukselle näkökulmia vaikka kuinka paljon. Haasteellisinta oli saada käsiteltyä tiiviisti mutta tarpeeksi informatiivisesti tärkeimmät pienen yrityksen tietoturvallisuuteen liittyvät asiat. Kirjoittamisen edetessä jouduin lisäämään työhöni monia asioita, joita en ollut alun perin suunnitellut, joten työ venyi kirjoitettaessa aika tavalla.

6 Lähteet

Järvinen, Petteri 2006. Paranna tietoturvaasi. Porvoo: Docendo. ISBN: 951-846-289-5

Kirves, Antti 2007. Tiedonhävitys on tekniikkalaji. Digitoday. [Online] [Viitattu 19.4.2007]. http://www.digitoday.fi/page.php?page_id=14&news_id=200313127

Laaksonen Mika, Nevasalo Terho, Tomula Karri 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita. ISBN: 951-37-4701-8

Microsoft Corporation 2007. Varmuuskopiointi voi pelastaa yrityksesi. [Online] [Viitattu 13.11.2007] http://www.microsoft.com/finland/pkinfo/issues/sgcv2/security-guidance-centre/Back-Up-Now-or-Be-Sorry-Later.mspx

Myhr, Bertil ym. 2004. Sulje ikkunasi kutsumattomilta vierailta. Symantec Corporation. ISBN: 91-975601-3-8

Ruohonen, Mika 2002. Tietoturva. Porvoo: Docendo. ISBN: 951-846-163-5

Teollisuuden ja Työnantajain Keskusliitto 2001. Ovatko yrityksesi tietoriskit hallinnassa? Uusitettu laitos. Helsinki: EK. ISBN: 951-9148-90-6

Thomas, Tom 2004. Verkkojen tietoturva. Cisco Press. Suomenkielinen painos. Helsinki: IT Press. ISBN: 951-826-780-4

Tero Tammisalo 2007. Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi. Periaatteet ja menetelmät. Helsinki: STAKES.

Wikipedia 2007. [Online] [Viitattu 13.11.2007]. http://en.wikipedia.org/wiki/Advanced_Intelligent_Tape

Wikipedia 2007. [Online] [Viitattu 13.11.2007]. http://en.wikipedia.org/wiki/Linear_Tape-Open

Microsoft Corporation 2007. Volume shadow copy overview. [Online] [Viitattu 14.11.2007] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ntbackup_backup_snapshot.mspx?mfr=true

Microsoft Corporation 2007. How Volume Shadow Copy Service Works. [Online] [Viitattu 14.11.2007] http://technet2.microsoft.com/windowsserver/en/library/2b0d2457-b7d8-42c3-b6c9-59c145b7765f1033.mspx?mfr=true