KOTIKÄYTTÄJÄN TIETOTURVA

Case: F-Secure Internet Security 2006

LAHDEN AMMATTIKORKEAKOULU
Liiketalouden koulutusohjelma
Yritysviestintäjärjestelmät
Opinnäytetyö
10.12.2006
Jukka Helin

Lahden ammattikorkeakoulu
Liiketalouden koulutusohjelma

HELIN, JUKKA:

Kotikäyttäjän tietoturva
Case: F-Secure Internet Security 2006

Yritysviestintäjärjestelmien opinnäytetyö, 52 sivua
Kevät 2007

TIIVISTELMÄ

Tämä opinnäytetyö käsittelee kotikäyttäjän tietoturvaa. Tutkimus selvittää kuinka yksittäinen tietokone voidaan suojata ja mitkä ovat ne riskit, jotka sen tietoturvaa uhkaavat. Tärkeä osa suojausta ovat tietoturvaohjelmat, joten tutkimuksessa vertaillaan neljää eri tietoturvaohjelmaa ja tuodaan esille minkälaisia ominaisuuksia ne sisältävät. Ominaisuuksiltaan ja käyttömukavuudeltaan kotikäyttäjälle sopivinta ohjelmaa F-Secure Internet Security 2006 testataan käytännössä ja tutkitaan miten vertailussa huomioidut asiat on toteutettu.

Tutkimuksen tarkoitus on selvittää, miten kotikäytössä oleva tietokone voidaan suojata tietoturvariskeiltä ja minkälaisilla toimenpiteillä suojaus voidaan toteuttaa.

Lähteinä työssä käytettiin alan kirjallisuutta, lehtiä ja Internetissä olevia artikkeleita. Lisäksi F-Secure Internet Security 2006 toimintaa tutkittiin käytännön toimintatutkimuksen menetelmin.

Tutkimuksen pohjalta voidaan todeta, että kotikäyttöön tarkoitetun tietokoneen suojaaminen on pitkä ja monivaiheinen, jatkuvaa ylläpitoa vaativa prosessi. Vaikka nykyiset suojaustyökalut, kuten F-secure Internet Security 2006 ovat erittäin kehittyneitä, eivät ne poista päävastuuta käyttäjältä. Suurin osa tietoturvaongelmista johtuukin juuri käyttäjän toimista.

Asiasanat: Tietoturva, Tietoturvaohjelma, Tietoturvauhka

Lahti University of Applied Sciences

Faculty of Business Studies

HELIN, JUKKA:

Home User’s Data Security
Case: F-Secure Internet Security 2006

Bachelor’s Thesis in Business Information Systems, 52 pages
Spring 2007

ABSTRACT

This thesis deals with the home user’s data security. The thesis discusses how a single computer can be protected and what are the threats it should be protected against. An important part of protection are data security programs, so the thesis compares four different programs and brings forth what kind of features they contain. F-Secure Internet Security 2006, the most suitable program for the home user as far as features and usage comfort are concerned, is tested in practise and its features are compared with those of the other programs.

The purpose of this thesis is to define how computers in home use can be protected against security threats and with what kind of actions it can be accomplished.

Sources used included books, magazines and articles on the Internet. Additionally the operating of F-Secure Internet Security 2006 was studied with the method of practical activity analysis.

From the results of the study, it can be stated that protecting a computer which is meant for home use has many phases and it is a long-term process which needs continual maintenance. Although the present protection tools, such as F-secure Internet Security 2006 are very advanced, they do not take the responsibility off from the user. Most of the security problems are in fact the result of the user’s actions.

Key words: Data security, Data security program, Data security threat

1 JOHDANTO

Laajakaistayhteydellä varustettu tietokone löytyy jo lähes jokaisesta nykyaikaisesta kodista. Suomalaiset ovat edelläkävijöitä uuden tekniikan käyttöönotossa ja suuri osa arkipäiväisistä toimista onkin siirtynyt verkkoon. Tietokonetta käytetään usein miettimättä sen kummemmin, miten ne toimivat. Tavallinen käyttäjä unohtaakin usein, että suojaamaton tietokone on avoin ovi esimerkiksi haittaohjelmille ja tietomurtautujille. Liian usein käyttäjä ymmärtää suojautumisen tärkeyden vasta sitten kun tietoturvaa on loukattu. Tietoturvasta onkin tullut osa jokaisen ihmisen arkipäivää. (Järvinen 2002, 21.)

Suojautumisen tarpeellisuus on helpompaa ymmärtää, kun tiedostaa olemassa olevat riskit. Tavallisimpia uhkia ovat olleet esimerkiksi erilaiset virukset sekä madot. Nämä uhkat pystytään kuitenkin torjumaan nykyisillä tietoturvaohjelmistoilla varsin tehokkaasti. Ongelmana ovatkin tietomurtautujien kehittämät uudet hyökkäystavat sekä uudenlaiset haittaohjelmat. Haittaohjelmien tekijöiden ja tietomurtautujien yleisin motiivi ei ole enää julkisuuden ja jännityksen haku vaan taloudellinen hyöty. Perinteinen rikollisuus, kuten uhkailu, varastaminen ja kiristys ovat siirtyneet verkkoon, sillä kiinnijäämisriski on verkossa oleellisesti pienempi. Nykyiset haittaohjelmat yrittävät asentua mahdollisimman salassa ja kerätä henkilökohtaisia tietoja käyttäjästä. Henkilökohtainen tieto, kuten sähköpostiosoitteet sekä luottokorttinumerot, ovat haluttua tavaraa rikollisten keskuudessa. Henkilökohtaista tietoa saatetaan jopa myydä eteenpäin roskapostittajille, rikollisille tai kelle tahansa maksavalle taholle. (F-Securen tietoturvakatsaus heinä-joulukuu 2006: hiljaisuus voi olla petollista, 2006.)

Vastuu tietokoneen suojaamisesta on käyttäjällä. Tärkeää on aina valmistautua pahanpäivän varalle eli muistaa ennaltaehkäisevä suojautuminen. Tämä tutkimuksen tavoite on selventää ne tekijät, joiden avulla tietokoneen suojaus uhkia vastaan on mahdollista toteuttaa. Tärkeää on ennaltaehkäiseminen, mutta myös tietää miten toimia tilanteessa, jossa ennalta odottamaton tietoturvauhka on jo toteutunut.

1.1 Tutkimuksen tavoitteet ja aiheen rajaus

Tässä opinnäytetyössä tutkitaan yksittäisen työaseman tietoturvaa. Tavoitteena on ohjata, kuinka yksityiskäyttäjän olisi viisainta suojata tietokoneensa ja selvittää ne riskit, joita vastaan tietokonetta oikeastaan suojataan. Työssä ei anneta yksityiskohtaisia ohjeita järjestelmän suojaamiseksi, vaan kerrotaan yleisesti erilaisista suojaustavoista, joita suojauksessa on mahdollista käyttää. Työssä esitetyt suojaustavat eivät ole ainoa ja oikea tapa suojata työasema. Tutkimuksessa keskitytään lähinnä laajakaistalla ja Windows XP käyttöjärjestelmällä varustettuihin työasemiin. Työssä sivutaan myös tietosuojaa, mutta pääpaino on tietoturvassa.

Tietokonetta suojatessa ovat tietoturvaohjelmistot tärkeässä roolissa, joten tässä tutkimuksessa verrataan useita eri tietoturvaohjelmistoja ja tuodaan esille, kuinka ne eroavat toisistaan. Käyttäjän onkin tarpeellista ymmärtää minkälaisia ominaisuuksia nykyiset tietoturvaohjelmistot sisältävät (Kaartinen 2006, 84).

Tavoitteena on löytää yksityiskäyttäjälle sopivin tietoturvaohjelmisto. Tutkimuksessa verrataan neljää tunnettua yksityiskäyttöön suunniteltua tietoturvaohjelmaa F-Secure Internet Security 2006, Symantec Norton Internet Security 2006, Panda Platinium 2006 Internet Security sekä McAfee Internet Security Suite 2006. Tärkeitä kriteerejä yksityiskäyttäjälle tietoturvaohjelmaa hankittaessa ovat hinta, tietoturvallisuus ja käytön helppous (Kaartinen 2006, 84). Näitä seikkoja pyritään painottamaan sopivinta tietoturvaohjelmaa valittaessa. Kun lähteiden perusteella sopivin ohjelmisto yksityiskäyttäjälle on valittu, suoritetaan toimintatutkimus siitä, kuinka valittu tietoturvaohjelmisto käytännössä vastaa sille asetettuja odotuksia. Toimintatutkimus on rajattu siten, että siinä tarkastellaan ainoastaan tietoturvaohjelman toimintaa.

1.2 Tutkimusongelma

Tämän opinnäytetyön tutkimusongelma on, kuinka yksityiskäytössä oleva työasema voidaan suojata tietoturvariskeiltä. Työssä käsitellään työaseman tietoturvauhat ja niiltä suojautuminen. Olennainen osa työaseman suojausta ovat tietoturvaohjelmat. Tietoturvaohjelmia on suuri määrä, joten työssä tutkitaan, mikä tietoturvaohjelmisto olisi yksityiskäyttöön sopivin tietoturvaratkaisu ja mitä ominaisuuksia ohjelmat sisältävät.

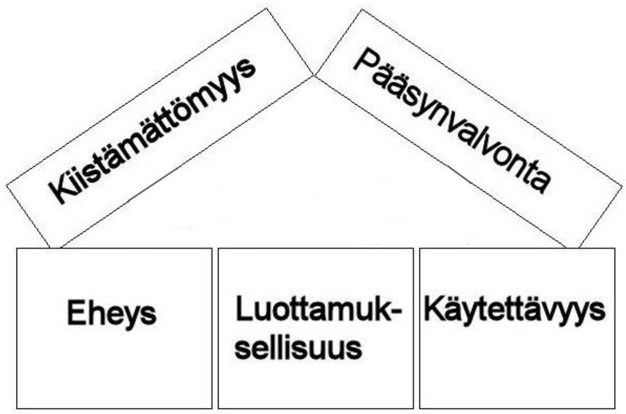
1.3 Tutkimusmenetelmät ja työnrakenne

Tämän opinnäytetyön tutkimusmenetelmä on empiirinen. Tutkimus voidaan jakaa kolmeen osaan. Ensimmäisessä osassa tutkitaan tietoturvan riskit ja suojautumiskeinot teoriassa, kirjallisia sekä verkkolähteitä apuna käyttäen. Toisessa osassa vertaillaan teoriatasolla neljää tietoturvaohjelmaa tietokonelehtien avulla. Kolmas osa on käytännön toimintatutkimus, jossa verrataan aiemmin tutkitun tiedon perusteella, onko valittu tietoturvaohjelma ominaisuuksiltaan aiemmin esiteltyjen huomioiden mukainen. Toimintatutkimus toteutetaan nykyaikaisella ja tehokkaalla suomenkielisellä Windows XP:llä varustetulla työasemalla.

2 TIETOTURVA

2.1 Tietoturvallisuuden määritelmä

Tietoturvallisuus on laaja ja usein vaikeasti hahmotettava kokonaisuus. Jotta tietoturvaa voidaan suunnitella, tarvitaan selkeä määritelmä tietoturvallisuudesta. Tietoturvallisuuden laajennetussa määritelmässä tietoturvallisuudella tarkoitetaan teknisiä ja hallinnollisia toimenpiteitä, joilla pyritään takaamaan tiedon luottamuksellisuus, eheys, käytettävyys, kiistämättömyys ja pääsynvalvonta (KUVIO 1). (Hakala, Vainio & Vuorinen 2006, 3-6.)



KUVIO 1. Tietoturvallisuuden osatekijät (Mukailtu lähteestä: Hakala ym. 2006, 6).

Luottamuksellisuudella tarkoitetaan sitä, että tietoa käsittelevät vain ne, joilla on siihen oikeus. Luottamuksellisuuteen pyritään suojaamalla tietojärjestelmän laitteet ja tietovarastot salasanoilla, käyttäjätunnuksilla ja salakirjoitusmenetelmillä. (Hakala ym. 2006, 3-6.)

Eheydellä tarkoitetaan, että tiedon käsittely taataan virheettömäksi eli tietojärjestelmän sisältämät tiedot pitävät paikkansa, eivätkä sisällä tahallisia tai tahattomia virheitä. Eheyteen pyritään ohjelmointiteknisillä ratkaisuilla. Sovelluksiin laitetaan erilaisia syötteen tarkistuksia tai syöttörajoituksia, tallennus- ja tiedonsiirto-operaatioihin varmistussummia tai tiivisteitä. Laitteistoissa pyritään virheet estämän käyttämällä esimerkiksi virheenkorjaavia muisteja tai väyliä. Tietoliikenneratkaisuissa suositaan virheen korjaus- ja tunnistusmekanismeilla varustettuja protokollia ja laitteita. (Hakala ym. 2006, 3-6.)

Käytettävyys tarkoittaa sitä, että tieto ja sen käsittelymekanismit ovat käyttäjien saatavilla, oikeassa muodossa ja riittävän nopeasti. Käytettävyyttä ylläpidetään huolehtimalla, että tieto- ja tietoliikennejärjestelmien laitteet ovat riittävän tehokkaita ja käytettävät sovellukset soveltuvia järjestelmään tallennettujen tietojen käsittelyyn. Tiedon jalostusta pyritään lisäksi automatisoimaan mahdollisimman pitkälle. (Hakala ym. 2006, 3-6.)

Kiistämättömyydellä tarkoitetaan järjestelmän kykyä tunnistaa ja tallentaa luotettavasti järjestelmää käyttävien henkilöiden tiedot. Tiedon kiistämättömyyteen pyritään lähinnä kahdesta syystä: halutaan varmistaa tiedon alkuperä tai olemassa olevien tietojen luvaton käyttö tilanteissa, joissa tietojärjestelmän omistaja joutuu harkitsemaan oikeudellisia toimia järjestelmän käyttäjää vastaan. Kiistämättömyyteen pyritään käyttämällä tunnistusmekanismeja ja biometrisiä tunnisteita. (Hakala ym. 2006, 3-6.)

Pääsynvalvonnalla tarkoitetaan menetelmiä, joilla rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä. Tietoturva pyrkii suojaamaan tärkeät tiedot ulkopuolisilta. Varsinaisiin tietoihin pääsyn rajoittaminen kuuluu luottamuksellisuuden ylläpitoon, mutta organisaatioille on kuitenkin tärkeää estää ulkopuolisia tai omaa henkilökuntaansa käyttämästä sen laitteita tai tietoliikenneyhteyksiä omiin tarkoituksiinsa. Luvattomat järjestelmän käyttäjät kuormittavat tietoliikenneverkkoja sekä laitteita ja heikentävät näin käytettävyyttä. Luvaton käyttö saattaa altistaa organisaation myös haittaohjelmien leviämiselle, mikä puolestaan johtaa eheys- sekä luottamuksellisuusongelmiin. (Hakala ym. 2006, 3-6.)

2.2 Tietosuoja

Tietoturvan lisäksi tulee myös huolehtia käyttäjän tietosuojasta. Tietosuojalla, jota kutsutaan myös yksityisyyden suojaksi, tarkoitetaan ihmisten henkilötietojen, sekä henkilökohtaiseen toimintaan liittyvien tietojen keräämisen ja käsittelyn rajoittamista siten, ettei henkilön yksityisyys turhaan vaarannu. (Järvinen 2002, 21.)

2.3 Mihin tietoturvaa tarvitaan?

Tietokonetta ja sen käyttäjää uhkaavat monet vaarat. Varsinkin verkkoon kytketty suojaamaton tietokone on aina alttiina tietoturvauhille, kuten verkkohyökkäyksille, viruksille ja madoille. Tietoturvan tehtävänä on varmistaa, että tietokoneet ja niissä olevat ohjelmat tekevät aina sen, mitä niiden on tarkoitus tehdä, eikä mitään muuta. Tietoturvaa tarvitaankin suojaamaan mahdollisimman monelta odotetulta ja odottamattomalta riskiltä. Lisäksi tietoturvaa tarvitaan varmistamaan, että järjestelmän suojattavat tiedot ovat vain niiden käyttöön oikeutettujen käyttäjien käytettävissä, ja että nämä tiedot ovat käyttäjien käytettävissä aina, kun he niitä tarvitsevat. (Ruohonen 2002, 2.)

3 TYÖASEMAN TIETOTURVAUHAT

3.1 Haittaohjelmat

Tietokoneohjelmien tarkoitus on auttaa käyttäjää. Ohjelmia käytetään työtehtäviin, viihdekäyttöön tai viestintään. Kaikki ohjelmat eivät kuitenkaan ole turvallisia, vaan voivat olla suorastaan vahingollisia. Haittaohjelmia ovat virukset, madot, Troijan hevoset ja vakoiluohjelmat. Haittaohjelmat toimivat samaan tapaan, kuin tavallisetkin ohjelmat, mutta niiden tarkoituksena on vahingoittaa tietokonetta ja sen käyttäjää. Haittaohjelmat voivat asentaa itsensä tietokoneeseen ja kopioitua jatkuvasti, jos tietokonetta ei ole suojattu. Nykyaikaisten ADSL yhteyksien yleistyttyä ovat haittaohjelmien aiheuttamat ongelmat lisääntyneet, kun moninkertainen tiedonsiirtonopeus mahdollistaa haittaohjelmien moninkertaisen leviämisen. (F-Secure Internet Security 2006 Opetusohjelma 2006.)

3.1.1 Virukset

Virus on haitallinen tietokoneohjelma, joka pystyy monistamaan itseään ja leviämään tietokoneesta toiseen. Virus ei kykene leviämään itsenäisesti, vaan se tarvitsee isäntätiedoston, jonka avulla se leviää ja aktivoituu. Virus aiheuttaa lähes aina avauduttuaan haittaa tietokoneelle ja siihen asennetuille ohjelmille. Useimmiten virukset pääsevät tietokoneelle sähköpostin liitetiedostoista tai Internetistä ladattujen tiedostojen kautta. Virustartunnan voi saada myös Web-sivustoilta, joilta työasema saa tartunnan. F-Securen mukaan vuonna 2000 viruksia oli liikkeellä 45 000. Vuonna 2004 virusten määrä on lisääntynyt 120 000:een. (F-Secure Internet Security 2006 Opetusohjelma 2006.)

3.1.2 Madot

Mato on samantapainen haitallinen tietokoneohjelma kuin virus. Mato on suunniteltu leviämään tietokoneesta toiseen automaattisesti. Mato leviää käyttäen hyväksi Internetiä ja käyttöjärjestelmien tietoturva-aukkoja. Mato leviää tietokoneesta toiseen nopeammin kuin virus. Madot jaetaan kahteen pääluokkaan, sähköpostimatoihin ja verkkomatoihin. (F-Secure Internet Security 2006 Opetusohjelma 2006.)

Sähköpostimadot käyttävät hyväkseen sähköpostiohjelmissa esiintyviä tietoturva-aukkoja. Ne keräävät sähköpostin osoitekirjaan tallennettuja sähköpostiosoitteita. Mato lähettää itsensä osoitteisiin, jotka osoitekirjaan on tallennettu, ja kerää mukanaan tietokoneesta tietoja ja liitetiedostoja. (F-Secure Internet Security 2006 Opetusohjelma 2006.)

Verkkomadot hyödyntävät palvelinohjelmissa olevia tietoturva-aukkoja. Ne monistavat itseään ja leviävät ilman aputiedostoja. Verkkomatojen suurin käyttäjälle näkyvä ongelma on niiden leviämisestä aiheutuva liikenne. Verkkomatotartunnan selvä merkki on, jos verkonsiirtonopeudet koneelta verkkoon ovat huomattavasti alhaisemmat kuin verkosta koneelle. Joskus verkkomadot saattavat kantaa mukanaan vaarallisia troijalaisia. (F-Secure Internet Security 2006 Opetusohjelma 2006.)

3.1.3 Troijan hevoset

Troijan hevonen on ohjelma, joka on naamioitu hyödylliseksi ohjelmaksi, mutta vahingoittaa tietokonetta käyttäjän tietämättä. Toisin kuin madot ja virukset, troijalaiset eivät pyri leviämään hallitsemattomasti, vaan niiden tarkoituksena on asentua mahdollisimman näkymättömästi. Troijan hevonen voi toimia itsenäisesti, kuten virus. Se voi olla esimerkiksi tietokonepeli, joka poistaa tietokoneesta tiedostoja pelin ollessa käytössä. Troijalainen saattaa toimia myös krakkerien hyökkäysvälineenä. Troijan hevosta, joka mahdollistaa ulkopuoliselle pääsyn tietokoneelle, kutsutaan takaoveksi. Takaovina toimivista Troijan hevosista ja niiden toiminnasta kerrotaan enemmän kohdassa 4.2 Krakkerien hyökkäysmuodot. (F-Secure Internet Security 2006 Opetusohjelma 2006.)

3.1.4 Vakoiluohjelmat

Vakoiluohjelma on haitallinen ohjelma, joka jäljittää käyttäjästä tietoja ja raportoi ne Internetiin sivullisille käyttäjän tietämättä. Yleensä vakoiluohjelma kerää tietoa Web-selauskäyttäytymisestä mainostarkoituksiin, mutta joskus se voi myös siirtää henkilökohtaisia tietoja ja tiedostoja tietokoneelta. Vakoiluohjelma saattaa seurata mitä näppäimistöllä kirjoitetaan, tai esimerkiksi muuttaa Web-selaimen kokoonpanoa. Vakoiluohjelmat hidastavat lisäksi verkon käyttöä, koska ne lähettävät tietoa käyttäjästä verkkoon. (F-Secure Internet Security 2006 Opetusohjelma 2006.)

3.1.5 Rootkit-ohjelma

Uusimpiin haittaohjelmiin kuuluvaa rootkit-ohjelmaa käytetään haitallisten ohjelmien piilottamiseen käyttäjältä. Kaikki rootkit-ohjelmat eivät ole sinällään haitallisia, mutta niitä voidaan käyttää haittaohjelmien, kuten virusten, troijalaisten ja matojen piilottamiseen. (F-Secure Internet Security 2006 Opetusohjelma 2006.)

3.2 Sähköpostin vaarat

Internet-sähköposti on mainio keksintö. Se on lähes ilmainen järjestelmä, joka siirtää tekstin ja liitetiedostot muutamissa sekunneissa. Sähköpostia voi käyttää myös melkein missä tahansa ajasta riippumatta. Sähköpostiin liittyy kuitenkin vaaroja ja tietoturvariskejä. Suurin osa Internetin haittaohjelmista leviääkin juuri sähköpostin kautta. (Järvinen 2002, 215.)

3.2.1 Roskaposti

Roskaposti on suurina määrinä lähetettyä kenellekään kohdistamatonta sähköpostia, jolle ei ole etukäteen saatu vastaanottajan lupaa. Roskaposti kuormittaa verkkoja ja tukkii sähköpostilaatikoita. Arvokasta aikaa kuluu roskapostien siivoamiseen. (F-Secure Internet Security 2006 Opetusohjelma 2006.) Lisäksi roskapostien mukana liikkuu usein vahingollisia sähköpostimatoja ja viruksia. Yleensä roskapostit lähetetään sellaisilta palvelimilta, jotka mahdollistavat postien todellisen lähettäjän henkilöllisyyden jäävän hämärän peittoon. Roskapostituksen määrää seuraavan Spamhouse-yrityksen perustajan Steve Linfordsin mukaan kaikesta sähköpostista 75–90% on roskapostia. Ongelmana on, että vain pienessä osassa maista roskapostitus on laitonta ja maissa, joissa lakeja on olemassa, on tuomioiden määrä pysynyt pienenä. Totuus on, että roskapostitus on hyvin helppoa, ja siitä on erittäin vaikeaa jäädä kiinni. (Wikipedia Roskaposti 2006.)

Joskus roskaposti voi olla myös tarkoituksella tietylle henkilölle kohdistettua. Tätä kutsutaan sähköpostipommitukseksi. Sähköpostipommituksessa krakkeri lähettää kohteelle valtavat määrät sähköpostia. Suuri määrä postia saattaa lamauttaa kohteena olevan käyttäjän sähköpostilaatikon. Sähköpostilaatikon kokoraja saattaa täyttyä, jolloin sähköpostipalvelin ei ota vastaan käyttäjälle lähetettyjä viestejä. Lisäksi sähköpostipalvelin saattaa hidastua tai mennä jopa lukkoon. (Ruohonen 2002, 355.)

3.3 Internetin vaarat

Internetiin pääsee kuka tahansa, eikä sieltä voi erottaa ketään. Satojen miljoonien verkonkäyttäjien joukkoon mahtuu rikollisia, huijareita ja häiriköitä. Nämä henkilöt eivät kaihda keinoja, vaan käyttävät hyödykseen sumeilematta Internetin porsaanreikiä. (Järvinen 2002, 179–183.)

3.3.1 Internet ja lapset

Lapset eivät vielä tiedä aikuisten maailman pelisääntöjä ja heidän persoonallisuutensa on vasta muodostumassa. Tästä syystä lapset on katsottu suojelua vaativaksi erikoisryhmäksi yhteiskunnassa. Internet on täynnä lapsille sopimatonta materiaalia. Ongelma onkin siinä, että miten rajoittaa alaikäisten pääsy sivuille, jotka on tarkoitettu aikuisille. (Järvinen 2002, 179–183.)

Verkon reaaliaikaiset keskustelualueet ovat vaarallisia, sillä koskaan ei voi tietää, onko keskustelija juuri se, joka väittää olevansa. 14-vuotiaana tyttönä esiintyvä saattaa olla todellisuudessa 50-vuotias mies. Tekstillä on helppoa hämätä, eikä mahdollinen valokuvakaan aina esitä oikeaa henkilöä. (Järvinen 2002, 179–183.)

3.3.2 WWW-selauksen tietoturvariskit

Jotkut sivujen ylläpitäjät yrittävät pitää verkonkäyttäjät Web-sivustoillaan väkisin tai haluavat tehdä muuten vain haittaa käyttäjälle ja hänen tietokoneelleen ja sortuvat kieroihinkin temppuihin. Sivuille saatetaan upottaa Java-, VBScript, Jscript ohjelmakieliä sisältävää materiaalia tai ActiveX-ohjelmia, joilla yritetään manipuloida käyttäjän selainta epämiellyttävällä tavalla. Esimerkkejä voivat olla sivuille piilotetut ohjelmat, jotka vaihtavat käyttäjän aloitussivun, pop-up-ikkunat, jotka aukeavat kun sivustolle tullaan tai kun sieltä yritetään poistua ja sivustot, jotka lisäävät itsensä kirjanmerkkeihin. Jotkut sivut estävät myös selaimen Back-painikkeen käytön. Pahimpia ovat haitalliset ActiveX-ohjelmat, jotka voivat tehdä tietokoneelle mitä tahansa, jos sellaisen erehtyy asentamaan. (Järvinen 2002, 199–201.)

3.3.3 Huijaukset

Huijarit käyttävät Internetiä uhrien metsästämiseen. Internetin välityksellä tarjotaan sijoituskohteita lomaosakkeisiin, IT-alan yrityksiin ja muihin pääomaa vaativiin kohteisiin. Useimmiten huijaukset tapahtuvat sähköpostin välityksellä, mutta niitä esiintyy myös Web-sivustoilla. Ehkäpä yleisimmin tunnettu huijaus on niin sanottu nigerialaishuijaus. Nigerialaishuijauksessa kenraali, virkamies tai joku muu merkittävässä asemassa oleva henkilö on saanut suuren summan rahaa ja tarvitsee sähköpostin vastaanottajan apua rahan siirtoon. Uhrille luvataan suurta summaa rahaa siitä, että hän taloudellisesti avustaa viranomaisten lahjomisessa ja rahansiirron käytännön järjestelyissä. (Järvinen 2002, 190.)

Toinen yleinen huijaus on Hoax, joka on sähköpostin kautta leviävä varoitus uudesta vaarallisesta ja olemattomasta viruksesta. Hoaxeille on tyypillistä, että väitetty virus aiheuttaa suurta tuhoa ja ettei yksikään virustentorjuntaohjelma tunnista virusta. Viestissä pyydetään levittämään virusvaroitusta mahdollisimman laajalle. Hoax-viesti on kuitenkin itsessään virus, joka leviää nopeasti erittäin suurelle alueelle. Hoax-viestissä on yleensä liitetiedosto, jonka väitetään olevan ainoa ohjelma, jolla viruksen voi torjua. Jos tällaisen liitetiedoston erehtyy avaamaan, virus aktivoituu. (Ruohonen 2002, 353.)

Yksi uusimmista huijaustavoista on Phishing-toiminta, joka tarkoittaa pankkitili- ja luottokorttitietojen varastamista sähköpostin avulla. Taidokkaasti laadittu Phishing -sähköpostiviesti lähetetään esimerkiksi Visa-, PayPal- ja eBay-asiakkaille. Viesti muistuttaa erehdyttävästi luottokorttiyritysten viestintää, ja käyttäjää yritetään ohjata sivuille, jotka ovat phishing -huijarien itsensä ylläpitämiä. Näillä sivuilla on kysymyksiä, joilla pyritään saamaan selville käyttäjän salaisia tilitietoja. (Symantec 2004, 28.)

4 VERKON TIETOTURVARISKIT

4.1 Hakkerit ja krakkerit

Sanat hakkeri ja krakkeri muistuttavat toisiaan kovasti eikä tavallinen käyttäjä usein tee eroa niiden välille. Yleensä hakkeri tai krakkeri ymmärretään henkilöksi, joka hyödyntää tietotekniikkaa rikollisiin toimiin. Hakkerilla ja krakkerilla on kuitenkin eroja. (Hakkerin käsikirja, 74.)

Hakkeri on henkilö, joka on kiinnostunut kaikesta tietokonekäyttöjärjestelmien vaikeaselkoisesta ja mutkikkaasta toiminnasta. Hakkerit ovat useimmiten ohjelmoijia, joten he ymmärtävät ohjelmoinnista ja käyttöjärjestelmistä. Hakkerit etsivät jatkuvasti tietoa ja jakavat selville saamiaan asioita muiden kanssa. Hakkerit eivät tuhoa tietoa tahallisesti. Hakkeria tietomurtoihin ja muihin laittomuuksiin ajaa useimmiten uteliaisuus, omien taitojen mittaaminen ja halu saada julkisuutta. Vaikka hakkerin toiminta voi olla harmitonta, on luvaton tunkeutuja aina tietoturvariski. (Hakkerin käsikirja, 74.)

Krakkeri tai kräkkeri on henkilö, joka murtautuu tietojärjestelmään ilman järjestelmän omistajan lupaa. Tällä tarkoitetaan esimerkiksi murtautumista verkon kautta kotitietokoneeseen. Krakkeri tekee tarkoituksella vahinkoa eikä epäröi jättää merkkiä käynnistään. Krakkerien motivaationa ovat vahingonilo ja oman edun tavoittelu eli raha. (Järvinen 2002, 295.)

Tässä opinnäytetyössä käytetään krakkeria yleisnimenä tietoturvauhkaa aiheuttavasta tietomurtautujasta.

4.2 Krakkerien hyökkäysmuodot

Krakkerit käyttävät erilaisia hyökkäysmuotoja päästäkseen käsiksi käyttäjän tietokoneeseen ja tietoihin. Hyökkäystapoja, joista yksityiskäyttäjän tulisi olla huolissaan, ovat muun muassa salakuuntelu, takaovet, palvelunesto, hajautettu palvelunesto ja murto. (Boström 2003, 45–60.)

Salakuuntelulla tarkoitetaan hyökkäystapaa, jossa hyökkääjä pyrkii tarkoituksella vakoilemaan sivullisten keskusteluja. Salakuuntelu on hyökkäysmuodoista teknisesti helpoin. Internetissä tieto kulkee datapaketteina useiden verkkolaitteiden kautta. Näitä laitteita ovat toistimet, kytkimet ja reitittimet. Salakuuntelua yrittävä krakkeri kytkee oman tietokoneensa verkkolaitteeseen, jonka läpi käyttäjän verkkoyhteydet kulkevat ja pystyy näin seuraamaan käyttäjän verkkoliikennettä. Vaarallisimmillaan krakkeri voi saada haltuunsa käyttäjän salasanoja ja käyttäjätunnuksia.(Boström 2003, 45–60.)

Eräs yleisimmistä hyökkäystavoista on haitallisen takaovi-ohjelman käyttäminen. Takaovesta on vaaraa vasta, kun käyttäjä käynnistää hyödylliseksi naamioidun ohjelman. Kun takaovi on asentunut tietokoneeseen, odottaa se komentoa verkosta tai ottaa yhteyttä toisaalla olevaan palvelimeen. Takaovet palvelevat kahdenlaisia tarkoitusperiä. Ensimmäisenä tarkoituksena on käyttää takaovea käyttäjän tekemisten seuraamiseen. Takaovi saattaa esimerkiksi tunnistaa käyttäjän näppäinpainallukset ja näin krakkeri saa kerättyä käyttäjätunnuksia ja salasanoja tulevia hyökkäyksiä varten. Toinen tarkoitus takaovelle on ottaa kone täydellisesti hallintaan, jolloin käyttäjän toimilla ei ole minkäänlaista vaikutusta. (Boström 2003, 45–60.)

Palvelunesto on hyökkäys, jonka tavoitteena on estää halutun sovelluksen, palvelimen tai kokonaisen verkon osan toiminta. Yleensä krakkeri hyödyntää ohjelmistojen tai käyttöjärjestelmien tietoturva-aukkoja, joiden kautta hän pyrkii kaatamaan käyttöjärjestelmän tai jumittamaan sovelluksia. Palvelunestohyökkäykset eivät usein kohdistu suoranaisesti yksityiskäyttäjän tietokoneeseen, mutta niistä on haittaa, kun krakkeri kaataa esimerkiksi www-palvelimen ja estää näin käyttäjältä pääsyn palvelimelle. (Boström 2003, 45–60.)

Eräät takaoven muodot tarjoavat hyökkääjälle mahdollisuuden käyttää useita ympäri verkkoa sijaitsevia koneita hyväkseen kohdejärjestelmän pommittamiseen. Tietokoneita, johon tällainen takaovi on asennettu, kutsutaan zombeiksi. Tämä hajautetuksi palvelunestohyökkäykseksi kutsuttu hyökkäysmuoto on nykyisin yleisin hyökkäystapa suuria palvelimia vastaan. Zombie koneista saatetaan myös kerätä kaikkea mahdollista yksityistä tietoa esimerkiksi roskapostittajien tarpeisiin. Kotikäyttäjälle vaara ei ole joutua hajautetun palvelunestohyökkäyksen kohteeksi vaan, että hänen tietokoneestaan tulee osa zombie-verkkoa. Zombie-verkkoa kutsutaan myös bottiverkoksi. (Boström 2003, 52–55)

Murto on hyökkäysmuodoista luultavasti tunnetuin. Murrossa krakkeri käyttää käyttöjärjestelmän tai ohjelmistojen tietoturva-aukkoja hyväkseen ja pyrkii pääsemään käsiksi käyttäjän koneen tiedostoihin. Koska yksittäisillä tietokoneilla on harvoin mitään krakkeria kiinnostavaa, ovat nämä hyökkäykset kuitenkin harvinaisimpia. Yleensä murrot kohdistetaan lähinnä yritysverkkoihin, joista yritetään vakoilla yrityssalaisuuksia. (Boström 2003, 45–60.)

4.3 Langattoman verkon tietoturvauhat

Langattomat verkot ovat suhteellisen uusia tuotteita kotikäytössä, ja verkkoa asentaessa unohtuukin usein se tärkein, eli verkon suojaaminen. Käyttäjä saattaa ajatella, että pelkkä langattoman verkon toimimaan saaminen riittää. Suurin turvariski langattomia verkkoja käytettäessä onkin niiden käyttäjä. Ongelma on, että langattomat verkot ovat erityisen alttiita tietoturvaloukkauksille. Langattomuus edellyttää aivan toisenlaista suojausta kuin perinteinen lankaverkko. Langatonta verkkoa on helpompi vakoilla ja siihen on helpompi hyökätä, kun krakkerin ei tarvitse päästä käsiksi verkkojohdon päässä olevaan verkkolaitteeseen, vaan kykenee langattomasti suorittamaan hyökkäyskomennot. WLAN yhteyteen on myös helpompi kytkeytyä, jolloin sitä voidaan käyttää luvattomasti. Kräkkerit saattavat käyttää ilman lupaa käyttäjän ADSL-yhteyttä tai murtautua tietokoneelle, jos yhteys on suojaamaton. (Hakala ym. 2006, 295–296.)

5 YMPÄRISTÖN AIHEUTTAMAT UHAT

5.1 Tilojen fyysinen turvattomuus

Yksi vakavimmista tietoturvaongelmista johtuu yleensä siitä, että ulkopuolinen henkilö pääsee liian helposti tilaan, jossa tietokone sijaitsee. Jos tietokonetta ei ole suojattu millään lailla, voi kuka tahansa tulla lukemaan sen tiedostoja, lähettämään sähköpostia koneen haltijan nimissä tai asentamaan koneeseen takaoviohjelmia. (Järvinen 2002, 49–50.)

5.2 Ympäristön aiheuttamat uhat

Tietokone on herkkä sähkölaite, joten se on altis ympäristöstä johtuville vaikutuksille. Tietokoneen altistuessa vedelle tai ilmankosteudelle, voi seurauksena olla laitteistovika. Tietokoneet ovat nopeilla prosessoreilla varustettuja aktiivilaitteita, jotka tuottavat huomattavan määrän lämpöä, joten huoneen lämpötilan liian suurien vaihtelujen seurauksena voi olla ongelmia. Esimerkiksi pöly ja epäpuhtaudet aiheuttavat lämmön nousua. Tuhoeläimet, kuten muurahaiset ja jyrsijät saattavat hakeutua ATK-laitteisiin, joka tulee ottaa huomioon alueilla, jossa niitä esiintyy. (Hakala ym. 2006, 304–311.)

5.3 Laitteiston uhat

Virran äkillinen katkeaminen tai hetkellinen alijännite saattavat aiheuttaa tietojen häviämisiä tai tahatonta muuttumista sekä fyysisiä laitevikoja. Tele- ja sähköverkoista voi tulla häiriötä. Pahimmillaan sähköinen häiriö voi olla salamanisku, joka saattaa jopa hajottaa tietokoneen tai siihen kytkettyjä laitteita. Kuten kaikki sähkölaitteet, saattaa tietokone tai sen osia hajota myös ilman näkyvää syytä. (Hakala ym. 2006, 304–311.)

6 HENKILÖTURVALLISUUDEN UHAT

Tietoturva ei rajoitu pelkästään tietokoneisiin. Oli kyseessä yksittäinen kotitietokone tai pieni kotiverkko muodostaa käyttäjäkunta aina suurimman uhan tietokoneen tietoturvalle. Valtaosa tietoturvaongelmista johtuu liian herkkäuskoisista tai välinpitämättömistä käyttäjistä. Yleisimmät nykykäytössä olevat käyttöjärjestelmät eivät ole oletusarvoisesti tietoturvallisia, joten käyttäjän omalla toiminnalla on suuri merkitys taistelussa tietoturvauhkia vastaan. Vaikka haittaohjelmat käyttävätkin tietoturva-aukkoja hyväkseen levitessään, on suurin syy niiden leviämiseen tietämätön tai laiska käyttäjä. (Boström 2003, 134–143.)

7 TYÖASEMAN SUOJAAMINEN

7.1 Virustorjunta

Viruksia, matoja, troijalaisia, rootkit-ohjelmia, ja muita haitallisia ohjelmia torjutaan virustorjuntaohjelmalla. Haittaohjelmiin kuuluvia vakoiluohjelmia ei yleensä torjuta virustorjuntaohjelmalla, vaan niitä vastaan on olemassa erillisiä vakoiluohjelman poistajia. Tietokoneessa, joka on jonkinlaisessa yhteydessä muihin tietokoneisiin verkkoyhteyden tai vaikkapa levykkeillä siirrettävien tiedostojen kautta, tulisi olla virustentorjuntaohjelma. Virustorjuntaohjelman pääasiallinen tehtävä on ennaltaehkäistä haittaohjelmien aktivoituminen ja tarvittaessa estää aktivoituneen haittaohjelman vahingollinen toiminta. (Ruohonen 2002, 226–227.)

Virustorjuntaohjelma eli virustutka voi etsiä haittaohjelmia käyttäjän suorittamalla niin sanotulla manuaalisella etsinnällä. Käyttäjän aktivoima manuaalinen tarkistus etsii haittaohjelmia tietokoneen keskusmuistista ja tiedostoista. Useimmissa virustorjuntaohjelmissa voi tarkistuksen myös ajastaa toimimaan automaattisesti tiettynä kellonaikana. Toista virustutkan käyttämää haittaohjelmien etsintätapaa kutsutaan aktiivisuojaukseksi. Se tarkistaa, että kaikki käyttäjän käsittelemät tiedostot ovat turvallisia, eikä niistä löydy haittaohjelmia. (Ruohonen 2002, 226–227.)

Virustorjuntaohjelmat tunnistavat haittaohjelmat kolmella eri menetelmällä. Ensimmäinen menetelmä on tunnettujen haittaohjelmien etsiminen. Tämä tarkoittaa sitä, että virustorjuntaohjelma etsii haittaohjelmien aina samana pysyviä osia, kuten tiettyä komentojen ryhmää. Toinen menetelmä on heuristinen tunnistusmenetelmä. Tässä menetelmässä virustorjuntaohjelma etsii haittaohjelman toimintaa muistuttavia piirteitä, kuten komentoja, joilla ohjelma kopioi osan omasta ohjelmakoodistaan toisen ohjelman loppuun. Koska heuristinen menetelmä ei etsi haittaohjelmia, vaan haittaohjelmia muistuttavia ohjelmia, saattaa se antaa vääriä hälytyksiä tai löytää uuden, ennen tuntemattoman haittaohjelman. Tällöin käyttäjän tulee itse todeta onko varoituksen aiheuttanut ohjelma haitallinen vai ei. Kolmas menetelmä on ohjelmien toiminnan seuraaminen. Tällä tarkoitetaan käynnissä olevien ohjelmien seuraamista. Kun ohjelma tekee jotain kiellettyä, kuten yrittää alustaa kovalevyn, estetään ohjelman suoritus. (Ruohonen 2002, 226–227.)

Virustorjuntaohjelma on tehokas vain, kun sen virustunnisteet ovat ajan tasalla. Virustunnisteilla tarkoitetaan tietokantaa, joka sisältää tiedon, jolla haittaohjelmat tunnistetaan ja poistetaan. Uusia haittaohjelmia tulee päivittäin lisää, joten virustorjuntaohjelma, jonka virustunnisteet ovat vanhentuneet, ei tunnista enää uusimpia haitallisia ohjelmia. Tästä syystä virustorjuntaohjelma tulisi päivittää ohjelman valmistaneen yrityksen palvelimilta Internetistä mahdollisimman usein. Useimmissa virustorjuntaohjelmissa on virustunnisteet päivittävä toiminto kokonaan automatisoitu, joten verkossa olevan tietokoneen virustunnisteet päivittyvät ilman käyttäjän toimia. Käyttäjän tulisikin varmistaa, että hänen virustorjuntaohjelmansa päivittyy oikein. (Ruohonen 2002, 226–227.)

7.2 Vakoiluohjelmien poistaja

Vakoiluohjelmien poistajat ovat samantyyppisiä ohjelmia, kuin virustorjuntaohjelmat. Vakoiluohjelmien poistajan tehtävänä on poistaa nimensä mukaisesti vakoiluohjelmia. Toisin kuin virustorjuntaohjelmissa, ei vakoiluohjelman poistajista löydy yleensä aktiivisuojausta, vaan vakoiluohjelmat etsitään manuaalisesti tarkistamalla. Kuten virustutkissa myös vakoiluohjelmien poistajissa on tärkeää, että vakoilutunnisteita päivitetään. Jokaisessa tietokoneessa tulisi olla vakoiluohjelmien poistaja, jotta käyttäjän tiedot eivät päätyisi ulkomaailmaan eikä verkkoliikenne tukkeutuisi. (Ylä-Jääski ym. 2006, 24–30)

7.3 Sähköpostin suojaaminen

Sähköpostin käyttöön liittyy paljon tietoturvariskejä ja se olisikin tärkeää suojata uhkia vastaan. Käyttäjällä onkin suuri vastuu sähköpostin suojaamisessa, sillä kaikkea sähköpostia koskevia suojauksia ei ole pystytty automatisoimaan. (Ruohonen 2002, 114–115.)

7.3.1 Suojautuminen vahingollisilta liitetiedostoilta

Sähköpostien mukana tulevat liitetiedostot muodostavat erityisen suuren riskin, sillä ne sisältävät usein haittaohjelmia. Käyttäjän tulisi olla varuillaan, jos liitetiedoston tiedostopääte on jokin seuraavista:exe (ohjelmatiedostot), scr (näytönsäästäjä), .vbs (Visual Basic Script), .bat (komentojono) ja .pif (Dos-ohjelmien kuvaustiedosto Windowsia varten). Joskus käyttäjää yritetään huijata avaamaan tiedosto, jossa on kaksi tiedostopäätettä peräkkäin, kuten tiedosto.txt.vbs. Tällä tekniikalla yritetään peittää tiedoston todellinen tiedostopääte, koska Windows Xp:n oletusasetuksilla eivät tiedostojen tiedostopäätteet ole näkyvissä.

Käyttäjän olisikin syytä laittaa tiedostopäätteet näkyviin Windowsin asetuksista, jotta näitä vahingollisia tiedostoja ei erehtyisi avaamaan. Viimekädessä tehokkain suoja haittaohjelmia vastaan on virustorjuntaohjelma, mutta kaikkein uusimpia viruksia vastaan ei siitäkään ole hyötyä. Jos käytössä on sähköpostiohjelma, olisi siihen syytä asentaa uusimmat tietoturvapäivitykset aina, kun se on mahdollista. (Järvinen 2002, 275–279.)

7.3.2 Roskapostilta suojautuminen

Roskaposti on yksi suurimmista sähköposteja vaivaavista ongelmista. Roskapostia vastaan on kuitenkin kehitetty suojautumiskeinoja. Paras tapa suhtautua roskapostiin on poistaa kaikki roskapostiksi epäilty posti tyynen rauhallisesti enempiä miettimättä. Roskapostiviestejä ei kannata avata, koska niissä voi olla upotettuja linkkejä www-sivuille, jolloin tieto viestin avaamisesta välittyy mainostajalle. (Järvinen 2002, 237–241.)

Myös haittaohjelmia saattaa esiintyä roskapostissa. Useissa sähköpostiohjelmissa löytyy lista osoitteista, joista tuleva posti tuhotaan automaattisesti. Tätä listaa kutsutaan sulkulistaksi. Kaikki tulevien roskapostien lähettäjät onkin hyvä lisätä sulkulistalle. Näin roskaposti ei pääse sähköpostilaatikkoon seuraavalla kerralla. Tosin tämä on työlästä ja auttaa harvoin oleellisesti, koska roskapostin lähettäjien sähköpostiosoite tuskin pysyy samana. (Järvinen 2002, 237–241.)

Myös sähköpostipommitukselta voidaan suojautua sulkulistalla. Roskapostia vastaan on kehitetty myös torjuntaohjelmia. Torjuntaohjelmat pyrkivät tunnistamaan ja poistamaan mainokset niissä esiintyvien avainsanojen tai ilmaisumuotojen perusteella. Sähköpostiohjelmissa saattaa olla omia sähköpostisuodattimia, jotka käyttäjän kannattaa kytkeä päälle. (Järvinen 2002, 237–241.)

7.4 Ohjelmistopäivitykset

Sovellukset ja käyttöjärjestelmät ovat laajoja kokonaisuuksia, joten niissä on väistämättä virheitä. Vakavia virheitä kutsutaan turva-aukoiksi, joita krakkerit ja haittaohjelmat käyttävät hyväkseen aiheuttaessaan vahinkoa. Ohjelmien säännöllinen päivittäminen onkin tarpeen, jotta ohjelmien omat virheet sekä löydetyt tietoturva-aukot saadaan korjattua. Päivittäminen on pitkälti käyttäjän vastuulla, mutta jotkut ohjelmat osaavat myös automaattisesti päivittää itsensä, kuten Windows XP, joka tarkistaa päivityksensä automaattisesti. (Järvinen 2002, 74–76.)

7.5 Suojautuminen Internetin vaaroilta

7.5.1 Lasten suojeleminen

Internet on täynnä lapsille sopimatonta materiaalia. Myös Internet-pedofiilit ovat kasvava ongelma. Tästä syystä on lapsia suojeltava. Lapsien Internetin käyttöä on myös syytä valvoa. Päävastuun lapsien suojelusta kantavat vanhemmat. Vanhempien tulisi tiedostaa Internetissä esiintyvät vaarat ja ohjeistaa lapsiaan Internetin käytössä. Hyviä ohjeita vanhemmille löytyy esimerkkisi Mannerheimin lastensuojeluliiton Internet sivuilta osoitteesta: http://www.mll.fi/. (Järvinen 2002, 182–184.)

Ohjeiden ja valvonnan lisäksi lapsia voidaan suojella erilaisilla suodattimilla. Tämä on myös helpoin tapa estää haitallisten sivujen käyttö. Suodatinohjelmia on useita sekä ilmaisia että kaupallisia, ja osa tietoturvaohjelmistakin sisältää jonkinlaisen suodatinohjelman. Näiden ohjelmien toimintaperiaate on sama: estää pääsy sivuille, joissa esiintyy haitallista sisältöä. Suodatinohjelmia kutsutaan myös lapsilukoiksi. (Järvinen 2002, 182–184.)

Haitallisiksi lasketaan sivut, jotka sisältävät rasistista, satanistista, pornografista ja päihteiden käyttöä sisältävää materiaalia. Suodatinohjelma estää pääsyn haitallisille sivuille käyttämällä erilaisia menetelmiä, joita ovat sulkulista, URL-osoite, sivun sisältö ja sivun kuvat. Sulkulistalla tarkoitetaan listaa kielletyistä URL-osoitteista, joihin pääsyn suodatinohjelma estää. URL-osoitteen estossa ohjelma estää pääsyn sivuille, joiden osoitteissa esiintyvät esimerkiksi sana ”adult” tai ”sex”. Sivun sisällön estossa suodatinohjelma tarkistaa sivun sisällön ennen sen näyttämistä selaimessa. Jos sivulla esiintyy kiellettyjä avainsanoja, sivua ei näytetä. Estosivun kuvien avulla toteutetaan tutkimalla sivuston kuvien väripintoja ja sävyjä. Jos sivulla esiintyy sävyjä, jotka tulkitaan alastonkuviksi, estetään sivulle pääsy. (Järvinen 2002, 182–184.)

Suodatinohjelmat käyttävät yhtä tai useaa estomenetelmää samanaikaisesti. Suodatinohjelmat eivät ole kuitenkaan täydellisiä, sillä ne ovat täysin sokeita. Esimerkiksi sivun sisällön suodatuksessa ohjelma ei pysty erottamaan, onko kyse seksipalvelusta vai seksivalistuksesta. Käyttäjän onkin syytä huomioida tämä, kun haluttu sivusto ei aukea, vaikka se ei sisältäisikään sopimatonta sisältöä. (Järvinen 2002, 182–184.)

7.5.2 Haitallisilta WWW-sivuilta suojautuminen

WWW-sivustoilla saattaa esiintyä haitallisia ohjelmia ja vahingollista ohjelmakoodia. Näiltä uhilta suojaudutaan yksinkertaisilla toimilla. Internet selaimen asetuksiin on syytä kiinnittää huomiota. Selaimesta löytyvät turvallisuusasetukset kannattaa asettaa tiukoiksi, jolloin haitalliset koodit ja ohjelmat eivät pääse aiheuttamaan vahinkoa. Useimmissa selaimissa on lisäksi asetus, jonka avulla eri sivustot voidaan jakaa eri ryhmiin, kuten luotettavat sivustot ja epäluotettavat sivustot. Nämä asetukset eivät kuitenkaan suojaa, jos selaimen tietoturvapäivitykset eivät ole ajan tasalla, joten käyttäjän on tärkeää huolehtia, että hänellä on käytössään uusin versio käytössä olevasta selaimesta. Lisäsuojaa voidaan saada erilaisilla ohjelmilla, jotka suojaavat selainta. Useissa tietoturvapaketeissa on WWW-sivustojen vaaroja tarkkaileva toiminto, joka estää haittakoodin ja haittaohjelmien toiminnan. (Ruohonen 2002, 107–108.)

Myös käytettävällä Internetselaimella on tietoturvan kannalta merkitystä. Tietoturvayhtiö Symantecin tekemän tutkimuksen mukaan 69 prosenttia tietomurto yrityksistä kohdistui Internet Explorerin tietoturva-aukkoihin. Lisäksi Internet Explorerin tietoturva-aukkojen paikkaaminen kesti muita selaimia pidempään. Onkin viisasta käyttää vaihtoehtoista Internetselainta, kuten Mozilla Firefoxia tai Operaa. (Verkkohyökkäys kotona, 9-10)

7.5.3 Huijauksilta välttyminen

Sähköpostia käytetään huijausvälineenä, joten käyttäjän tulisi pitää varansa kaikkia tuntemattomia lähettäjiä kohtaan. Myös tuntemattomilla Web-sivustoilla esiintyviin tarjouksiin kannattaa suhtautua epäilevästi. Sähköpostin lähettäjänimen väärentäminen on nykyisin todella helppoa, joten kaikkiin sähköpostiin tuleviin viesteihin tulee suhtautua aina varauksella. Tärkeää on muistaa, että liian hyvä tarjous ei luultavasti ole totta. Huijarin tunnistaa usein kirjoitusvirheistä, englanninkielestä ja puutteellisista yhteystiedoista. Omia tietoja, kuten luottokorttitietoja tai tilinumeroita ei kannata antaa kellekään Internetin välityksellä. Terve maalaisjärki on aina valttia, mutta myös tietoturvasivuilta on viisasta hankkia tietoa huijarien käyttämistä huijaustekniikoista. (Järvinen 2002, 190.)

7.6 Kannettavien tietokoneiden tietoturva

Kannettavat tietokoneet aiheuttavat tietoturvalle haasteita. Pöytäkoneista poiketen kohdistuu kannettaviin tietokoneisiin suurta fyysistä rasitusta, kun niitä liikutellaan. Rasituksesta johtuen laitteistorikot ovat kannettavissa tietokoneissa paljon yleisempiä kuin pöytäkoneissa. Koska, kannettavia tietokoneita kuljetetaan usein mukana, ovat ne myös alttiimpia ympäristöstä johtuville vaaroille. Kannettavia tietokoneita myös varastetaan paljon. Varkaiden lisäksi kannettavia tietokoneita hukataan ja unohdetaan. Kannettavan tietokoneen omistajan on tärkeää olla huolellinen varsinkin silloin, kun hän ottaa tietokoneen matkalle mukaan. Kannettava tietokone on viisasta suojata salasanoilla, joita ei helposti voida murtaa varsinkin, jos tietokoneella säilytetään arkaluontoista materiaalia. Kannettavat mahdollistavat tietokoneen liikuttamisen verkosta toiseen. Vieraissa verkoissa, kuten nettikahvilan langatontaverkkoa käyttäessä on tärkeää muistaa asettaa palomuurin asetukset tiukoiksi, sillä kuka tahansa verkkoon kytkeytynyt voi helposti murtautua heikosti suojattuun tietokoneeseen. (Järvinen 2002, 79–94.)

7.7 Tiedonsalaus

Salausmenetelmillä pyritään varmistamaan tietojen luottamuksellisuus, eheys ja kiistämättömyys. Riippumatta siitä, mihin salausta käytetään, tavoitteena tulisi olla salaus, jonka murtaminen kohtuullisessa ajassa ja kohtuullisin resurssein ei ole mahdollista. Salattavan tiedon tärkeydestä riippuu, miten pitkä kussakin tapauksessa on kohtuullinen aika ja mitkä ovat kohtuulliset resurssit. (Boström 2003, 104–105.)

Tietokoneella saatetaan säilyttää salaista tai arkaluontoista materiaalia, jota ei haluta päästää ulkopuolisten käsiin. Tällainen materiaali on syytä suojata erillisellä salauksella. Salaus on matemaattinen ja looginen menetelmä, jossa alkuperäinen tieto muokataan salausalgoritmin ja salausavaimen avulla täysin tunnistamattomaksi. Salattu materiaali saadaan esiin ainoastaan avaimella, jota käytettiin tiedostoa salattaessa. Tiedon salaustapoja ovat muun muassa tiedostojärjestelmään perustuva salaus ja salausohjelman avulla tehtävä salaus. (Boström 2003, 104–105.)

Yleisin tapa suojata tiedostoja on käyttää salaavaa tiedostojärjestelmää. Esimerkiksi Windows XP:ssä käytetään NTFS tiedostojärjestelmää, joka mahdollistaa tietojen salaamisen. Tiedostojärjestelmään perustuva salaus on integroitu käyttöjärjestelmään ja tiedoston salaamiseen riittääkin sen asetuksien muuttaminen. Salausta käytettäessä ei tarvitse itse määritellä salasanoja, sillä käyttöjärjestelmä luo itse tarvittavat tiedostokohtaiset salausavaimet. Salaus on integroitu käyttöjärjestelmään siten, että avaimet salataan tiedoston omistajan julkisella avaimella ja puretaan hänen salaisella avaimellaan. Näin vain tiedoston salannut käyttäjä pystyy avaamaan salaamansa tiedoston. Tiedostojärjestelmään perustuvassa salaustavassa on kuitenkin huomioitava, että siirrettäessä salattuja tiedostoja esimerkiksi levykkeelle käyttöjärjestelmä purkaa salauksen automaattisesti. (Järvinen 2002, 82–84.)

Salaus voidaan suorittaa myös käyttämällä erillistä salausohjelmaa, kuten sähköpostien salaukseen tarkoitettua ilmaista Pretty Good Privacyä. Tämä ohjelma perustuu siihen, että lähettäjä salaa viestin avaimella ja viestin vastaanottaja purkaa sen. Näin varmistetaan se, että viestin päätyessä vääriin käsiin, ei sitä voi lukea ilman salausavainta. (Boström 2003, 107–108.)

7.8 Varmuuskopiointi

Varmuuskopiointi tarkoittaa tiedostojen kopioimista siltä varalta, että alkuperäinen kopio tuhoutuu. Tietokoneen komponentit hajoavat helposti ikääntyessään. Varsinkin kiintolevyt ovat tunnetusti vaurioherkkiä. Myös erilaiset haittaohjelmat ja käyttäjän oma huolimattomuus saattavat vaarantaa tietokoneessa olevat tiedot. Tästä syystä on hyvä varmuuskopioida kaikki tärkeät tietokoneesta löytyvät tiedostot, kuten työasiakirjat ja valokuvat. Windows XP:stä löytyy varmuuskopiointiohjelma, jolla voidaan varmuuskopioida tietokoneen tiedostot ja asetukset talteen ja palauttaa ne tarvittaessa. Varmuuskopio on syytä tallentaa varmaan paikkaan, kuten DVD-levylle tai toiselle kiintolevylle, josta tiedot voi palauttaa tarvittaessa, vaikka tietokoneeseen tulisikin laitevika tai jokin muu ongelma. (Ruohonen 2002, 209–219.)

8 VERKON SUOJAAMINEN

8.1 Palomuuri

Laajakaistayhteyksien yleistyttyä on palomuurista tullut välttämätön suoja tietokoneelle, joka on kytketty julkiseen verkkoon. Palomuuri on joko ohjelmistolla tai laitteistolla toteutettu järjestelmä, jota käytetään verkkotason pääsynvalvontamekanismina tiettyä verkkoa tai verkkoja varten. Palomuurin tärkein tehtävä on estää ulkopuolisten pääsy sisäiseen verkkoon, mutta sitä käytetään myös sisäverkosta ulkoverkkoon kulkevan liikenteen valvontaan. Ilman palomuuria voivat esimerkiksi troijalaiset ottaa vapaasti yhteyden krakkerin ylläpitämään palvelimeen. (Hakkerin käsikirja 2002, 199–200.)

Verkossa olevat laitteet käyttävät keskenään liikennöintiin TCP/IP -protokollaa. TCP/IP -protokolla sisältää tiedonsiirtoon tarkoitetut TCP-, ICMP ja UDP -protokollat, joihin kaikki käyttäjien ja tietokoneiden välinen liikenne perustuu. TCP- ja UDP -protokolla käyttävät portteja eri yhteyksien erottelemiseen. ICMP -protokolla ei tarvitse yhteyksien erotteluun portteja lainkaan. Portit ovat eräänlaisia kanavia, jotka voidaan avata ja sulkea palomuurin avulla. (Hakkerin käsikirja 2002, 201–209.)

Tietokoneelle asennetut sovellukset käyttävät eri portteja siirtäessään ja vastaanottaessaan tietoa, kuten Internet-selaimet, jotka käyttävät tiedonsiirtoon TCP -protokollan porttia 80. Palomuurit päättävät määrätyn sääntöjoukon perusteella, pitääkö portin läpi menevä verkkoliikenne sallia vai ei. Sääntöjoukko määräytyy käyttäjän päättämien palomuuriasetusten perusteella. Vain sallitut yhteydet pääsevät portin läpi, muut yhteyspyynnöt hylätään. (Hakkerin käsikirja 2002, 201–209.)

Palomuurin asetuksia muuttaessa on oltava tarkkana, sillä yksikin väärä sääntö voi tehdä palomuurista käyttökelvottoman. Tietokoneen kaikki verkkoliikenne kulkee palomuurin läpi ja se päästää lävitseen vain sallitun verkkoliikenteen. (Hakkerin käsikirja 2002, 201–209.)

Palomuuria voidaan käyttää myös tietoliikenteen seuraamiseen. Esimerkkinä voidaan mainita erilaiset tapahtumalokit ja hälytystoiminnot, joiden avulla tulevaa ja menevää tietoliikennettä voidaan seurata. (Hakkerin käsikirja 2002, 199–200)

8.1.1 Sovelluspalomuuri

Sovelluspalomuuri on ohjelmisto, joka asennetaan tietokoneeseen. Se valvoo käyttöjärjestelmän ja sen ohjelmien yhteydenottoja. Sovelluspalomuurin päätehtävä on estää asiattomat yhteydenotot Internetistä, sekä matojen, virusten ja vakoiluohjelmien aiheuttama haitallinen verkkoliikenne kotikoneelta ulkoverkkoon. Sitä voidaan lisäksi käyttää verkkoliikenteen valvontatyökaluna. Sovelluspalomuurilla heikkous on, että se on tavallinen tietokoneohjelma. Tästä syystä voidaan se sammuttaa ohjelmallisesti tai jopa kiertää. Eräät virukset ja madot pyrkivät jopa poistamaan olemassa olevat palomuuriasennukset. Uhkakuvista huolimatta antavat sovelluspalomuurit oikeinkäytettyinä varsin tehokkaan suojan. (Boström 2003, 66.)

8.1.2 Palomuurilaite

Palomuurilaite on fyysisesti erillinen laite, joka kytketään tietokoneen ja ulkoverkkoon liikennöivän laitteen, kuten ADSL-modeemin väliin. Palomuurilaitetta kutsutaan myös rautapalomuuriksi. Palomuurilaiteen tehtävä on sama, kuin sovelluspalomuurinkin eli asiattomien yhteydenottojen estäminen sisä- ja ulkoverkosta. Rautapalomuurin etu on, että sen kiertäminen tai sammuttaminen on hyvin hankalaa. Palomuurilaite voi lisäksi valvoa usean tietokoneen liikennettä ulkoverkkoon. Kotikäyttöön rautapalomuuri on oiva ratkaisu, varsinkin, jos käytössä on useampi, kuin yksi tietokone, koska sillä voidaan suojata useita tietokoneita kerralla. Rautapalomuuri on sovelluspalomuuria kalliimpi tietoturvaratkaisu, mutta antaa huomattavaa lisäsuojaa. (Boström 2003, 67–70.)

8.2 Langattoman verkon suojaus

Langattomanverkon suojaamiseksi on suunniteltu useita suojausmenetelmiä sekä liikenteen salakuuntelun että verkon luvattoman käytön ehkäisemiseksi. Yksityiskäytössä yleisimmät suojaukset ovat WEP -protokolla ja WPA -protokolla. Käytettävän tukiaseman ominaisuudet määräävät käytettävän salauksen. (Hakala ym. 2006, 293–297.)

WEP -protokolla eli Wired Equivalent Privacy – protokolla (WEP) on perusmekanismi, jolla pyritään turvaamaan verkkoliikenteen turvallisuus. WEP perustuu verkkokortteihin ja tukiasemiin määriteltyihin salausavaimiin. Käytettävien avainten enimmäispituus on 128 bittiä. Salausta tehtäessä on tärkeää valita mahdollisimman vahva salaus. Salauksessa käytetään yhtä avainta. Tämä mahdollistaa salauksen murtamisen erillisellä murto-ohjelmistolla, eikä harjaantuneella krakkerilla kestä kauaakaan murtaa WEP avainta. WEP avaimen tarjoamaa suojaa voidaan parantaa määrittämällä tukiasemaan lista oikeutetuista Mac-osoitteista, mutta tämä ei ole riittävä suojatoimenpide, sillä nykyisiin verkkokortteihin voidaan määritellä laitteen käyttämä Mac-osoite. WEP salausta onkin arvosteltu voimakkaasti sen sisältämien heikkouksien vuoksi. Puutteistaan huolimatta WEP on usein tavallisessa kotikäytössä riittävä suojatoimenpide. (Hakala ym. 2006, 293–297.)

WPA -protokolla eli Wireless Fidelity Protected Access-protokolla on edistyksellisempi versio WEP -protokollasta. WPA on tarkoitettu korvaamaan WEP -protokollan puutteita. Perusperiaatteeltaan WPA -protokolla on samanlainen kuin WEP -protokolla, mutta käytettävää salausavainta muutetaan automaattisesti lyhyin väliajoin, joten se tarjoaa paljon parempaa suojaa. Myös WPA salauksessa on heikkouksia, mutta langattoman verkon tukiasemaa valittaessa kannattaa aina valita WPA suojausta tukeva tukiasema. (Hakala ym. 2006, 293–297.)

9 YMPÄRISTÖN AIHEUTTAMILTA UHILTA SUOJAUTUMINEN

9.1 Fyysinen pääsynvalvonta

Tietokoneen tietoturva alkaa sen fyysisestä koskemattomuudesta. Kaikki turvatoimet ovat turhia, jos tietokoneen lähettyvillä liikkuu ulkopuolisia henkilöitä, jotka pääsevät käyttämään tietokonetta vapaasti. Tietokoneen turvaamista tämänkaltaisilta väärinkäytöksiltä kutsutaan fyysiseksi pääsynvalvonnaksi. Helpoin tapa turvata tietokoneen fyysinen koskemattomuus on säilyttää sitä lukitussa tilassa, johon muilla ei ole mahdollisuutta päästä. Tämä ei ole kuitenkaan aina mahdollista ja murtautumisen mahdollisuus fyysisesti ja verkon kautta on aina olemassa. Tästä syystä on tietokoneelle luotava salasanoja. (Järvinen 2002, 49–50.)

Tavallinen tapa turvata fyysinen pääsynvalvonta on käyttää erilaisia salasanoja. Ensimmäiseksi tulee huolehtia Windowsiin kirjautumissalasanasta, joka kysytään jokaiselta käyttäjältä Windowsin käynnistyessä. Myös sähköposti tulee suojata salasanalla. Nämä suojaukset riittävät useimmille käyttäjille, mutta jos haluaa olla täysin varma, etteivät ulkopuoliset pääse käyttämään tietokonetta on syytä lisätä BIOS-käynnistyssalasana. BIOS-käynnistyssalasanalla huolehditaan siitä, etteivät ulkopuoliset pääse muuttamaan BIOS:in asetuksia eivätkä käynnistämään tietokonetta omilla levykkeillä tai cd-levyillä. Kun tietokonetta ei käytetä, on syytä suorittaa tietokoneen lukitseminen. Tällä toimenpiteellä estetään luvaton käyttö käyttäjän ollessa poissa tietokoneen äärestä. Lukitseminen voidaan myös automatisoida käyttöjärjestelmän asetuksista. Jos tietokoneella on pääkäyttäjän lisäksi muita käyttäjiä, on tärkeää luoda heille omat käyttäjätunnukset rajoitetuilla oikeuksilla. Näin vierailevat käyttäjät eivät pääse esimerkiksi asentamaan omia ohjelmistojaan tietokoneelle, sillä kaikki ylimääräiset sovellukset muodostavat tietoturvariskin. Tämä toimenpide estää myös monien haittaohjelmien pääsyn tietokoneelle. (Järvinen 2002, 49–55.)

Salasana on tehokas tietoturvan parantaja, mutta hyvän salasanan keksiminen ei ole helppoa. Salasana onkin syytä miettiä huolella. Salasana ei saa olla henkilökohtaiseen elämään liittyvä, kuten lasten tai lemmikin nimi. Salasanan tulee olla pituudeltaan riittävän pitkä, jotta murto-ohjelmalla, joka kokeilee jokaisen vaihtoehdon yksi kerrallaan, ei saada sitä murrettua. Hyvä salasana sisältää isoja ja pieniä kirjaimia sekä erikoismerkkejä ja se on keinotekoisesti luotu kirjainsekamelska. Salasanoja käyttäessä on syytä muistaa, että jokaiseen käytettävään palveluun on keksittävä oma salasana. Vaikka yksi salasana saataisiinkin murrettua, ei murtautujalla ole oikeutta muihin käyttäjän palveluihin. Salasanat tulee muistaa vaihtaa uusiin säännöllisin väliajoin. Tärkeää on myös salasanan säilytyspaikka. Jos salasana jätetään näkyvälle paikalle tietokoneen viereen, ei siitä ole hyötyä. (Järvinen 2002, 339–343.)

9.2 Ympäristöturvallisuus

Ympäristön aiheuttamien uhkien välttämiseksi on syytä suunnitella tietokoneen sijoitus tarkkaan. Tietokone on viisasta sijoittaa paikkaan, jossa se ei altistu kosteudelle tai kuumuudelle. Myös tietokoneen puhtaudesta on syytä huolehtia. Pölyt on viisasta imuroida tietokoneen läheisyydestä ja tarvittaessa kotelon sisältä ainakin kerran kuussa. Tietokoneen kotelo on myös mahdollista suodata pölysuodattimilla. Jos tiedossa on, että tilassa jossa tietokone on, tai sen läheisyydessä, on tuhoeläimiä, kannattaa tietokone sijoittaa siten, että tuhoeläimet eivät pääse siihen käsiksi. Myös perinteisillä tuholaisten torjuntakeinoilla, kuten muurahaisrasioilla, voidaan tuhoeläimien aiheuttamilta vahingoilta välttyä. (Hakala ym. 2006, 304–307.)

9.3 Laitteistoturvallisuus

Jotta laitteisto toimisi, on huolehdittava sähkön aiheuttamista ongelmatilanteista. Yritykset käyttävät yleensä palvelinten ja kriittisten työasemien suojaamiseksi UPS-laitteita (Uninterruptible Power Supply), jotka antavat varavirtaa sähkökatkoksien sattuessa ja suojaavat jännitteen muutoksilta. UPS-laitteet ovat kuitenkin kalliita ja tästä syystä ne eivät ole vielä kotikäytössä suosittuja. UPS-laitteiden hinnat ovat kuitenkin laskeneet huomattavasti viime vuosina, joten nykyisin voi UPS-laite olla suositeltava vaihtoehto myös yksityiskäyttöön. Halvempi vaihtoehto UPS-laitteelle ovat erilaiset jännitesuojat. Jännitesuojan saa edullisesti ja se suojelee tietokonetta tehokkaasti jännitteen muutoksilta. Virran katketessa kokonaan ei jännitesuojasta ole kuitenkaan apua. (Hakala ym. 2006, 308–311.)

Tietokoneessa tapahtuviin laitteistojen hajoamisista johtuviin uhkiin voidaan varautua seuraamalla erilaisia diagnostiikkaohjelmia, jotka kertovat laitteiden tilasta. Esimerkiksi kiintolevyn rikkoontumista vastaan on kehitetty S.M.A.R.T, joka on lyhenne sanoista Self-monitoring, Analysis and Reporting Technology. Tämä laitteistoon integroitu tekniikka on kehitetty arvioimaan milloin käytössä oleva kiintolevy on tulossa käyttöikänsä päähän. Kun S.M.A.R.T ilmoittaa vakavista virheistä, on viisasta tehdä varmuuskopio kaikista tärkeistä tiedostoista ja vaihtaa kiintolevy. (Järvinen 2002, 97–99.)

10 HENKILÖTURVALLISUUS

Tietokoneen suurimman tietoturvauhan muodostaa käyttäjä itse. Tästä syystä jokaisen käyttäjän tulisi olla perillä tietoturvaan liittyvistä perusasioista. Tietoturvan opiskelu on hyvä aloittaa kirjallisuudesta tai Internetistä esimerkiksi kansalaisen tietoturvaoppaasta, joka löytyy sivulta: http://www.tietoturvaopas.fi. Tietoturvaopas tarjoaa perustietoa tietoturvasta jokaiselle käyttäjälle. Tietoturvassa tärkeintä ei kuitenkaan ole turvallisten menetelmien oppiminen vaan tietynlaisen vainoharhaisen asenteen omaksuminen. Käyttäjän tulisi oppia ymmärtämään, mitä tietoturvaa uhkaavia vaaroja on olemassa ja kuinka niiltä voidaan suojautua. Pelkkä tieto ei kuitenkaan riitä, sillä opittuja toimintatapoja täytyy oppia soveltamaan myös käytännössä kaikissa tietokoneisiin liittyvissä tilanteissa. Terveellä harkintakyvyllä ja rehellisellä maalaisjärjellä pärjääkin pitkälle. (Boström 2003, 134–144.)

11 KUN SUOJAUKSET PETTÄVÄT

11.1 Haittaohjelmatartunnasta toipuminen

Tavallisesti virustorjuntaohjelma ja haittaohjelmien poistajat huolehtivat haittaohjelmien poistamisesta. Joskus voi kuitenkin tulla tilanne, jossa haittaohjelmien poisto-ohjelmat eivät löydä tai osaa poistaa havaittuja haittaohjelmia, vaikka ne olisikin päivitetty uusimmilla ohjelmaversioilla ja haittaohjelmatunnisteilla. Tällaisessa tilanteessa kannattaa hakea apua tietoturvaohjelmien valmistajien sivuilta. Valmistajien sivustoilta löytyy ilmaisia haittaohjelmien etsintä- ja poistotyökaluja. Jos haittaohjelma on aiheuttanut vahinkoa jo siinä määrin, että järjestelmä ei toimi tai halutaan varmistaa, että haittaohjelma on varmasti poistunut tietokoneelta, on syytä suorittaa kovalevyjen täydellinen tyhjennys ja käyttöjärjestelmän uudelleenasennus. Tällaisessa tilanteessa korostuu varmuuskopioinnin merkitys, kun uudelleenasennuksessa menetetyt tiedot voidaan palauttaa varmuuskopiosta puhtaaseen työasemaan. (Ruohonen 2002, 228–229.)

11.2 Kun koneelle on murtauduttu

Murtautumisen voi huomata monesta seikasta. Mikäli palomuurin lokeista havaitaan suuria määriä lähtevää ja tulevaa verkkoliikennettä tai muita outoja verkkoon tai järjestelmään liittyviä tapahtumia on syytä epäillä, että tietokoneelle on murtauduttu. Tällaisessa tilanteessa on erittäin tärkeää toimia oikein. Hyökkääjät ovat murtautuneet tietokoneelle alun perin verkon kautta. Tästä syystä ensimmäisenä on tärkeää irrottaa tietokone fyysisesti verkosta. Käytännössä tämä tapahtuu irrottamalla verkkojohto tietokoneen verkkokortista. Tämän jälkeen kannattaa ottaa tuoreet varmuuskopiot tietokoneen sisältämistä tärkeistä tiedostoista. Seuraavaksi kartoitetaan mitä kautta tunkeutuja on päässyt tietokoneelle. Kaikki virustorjuntaohjelmat ja vakoiluohjelman poistajat kannattaa ajaa, jotta mahdolliset takaovet löytyisivät. Palomuurin lokeja tutkimalla voi kokenut käyttäjä löytää portit, joiden kautta murtautujat pääsevät tietokoneelle. Kun portit on paikallistettu, on ne syytä tukkia. Jos nämä toimenpiteet eivät kuitenkaan auta, vaihtoehdoksi ei jää muuta kuin tietokoneen täydellinen uudelleenasennus. (Boström 2003, 145–152.)

12 TIETOTURVAOHJELMAT

12.1 Mikä tietoturvapaketti on?

Tietoturvaohjelmaksi kutsutaan ohjelmia tai ohjelmistokokonaisuuksia, joiden tehtävänä on suojata työasemaa tietoturvariskeiltä. Tietoturvaohjelmia ovat esimerkiksi palomuuri, virustorjunta, vakoiluohjelmienpoistaja ja lapsilukko. Tietoturvaohjelma saattaa olla myös useita tietoturvaohjelmia sisältävä ohjelmistokokonaisuus. Tällaista ohjelmaa kutsutaan tietoturvapaketiksi. Tietoturvapaketin perusominaisuuksia ovat virustorjunta ja palomuuri. Muut sovellukset, kuten lapsilukko ovat tietoturvapaketin lisäominaisuuksia. (Tietoturvaopas tietoturvaohjelma 2006.)

12.2 Millainen on hyvä tietoturvapaketti?

Tietoturvapaketti on yleensä kaupallinen tuote, josta on maksettava, mikäli sellaisen tietokoneelleen haluaa. Tärkeää onkin valita tietoturvapaketti tarkkaan, sillä vaihtoehtoja on paljon. Hyvä tietoturvapaketti sisältää virustorjunnan automatisoitavalla ajastuksella ja palomuurin, jonka viestit ovat selkeitä. Virustorjunnan ja palomuurin lisäksi on tärkeää, että paketti sisältää myös muita ominaisuuksia, kuten roskapostinsuodatus ja lapsilukko. Parhaimmillaan tietoturvapaketin toiminta on hyvin läpinäkyvää, eikä käyttäjän tarvitse puuttua sen toimintaan kuin harvoin. Ohjelmiston olisikin syytä pitää itsensä automaattipäivitysten avulla ajan tasalla ilman käyttäjän toimia. Tietoturvapaketin käyttöönoton ja käytön tulee olla selkeää ja havainnollista. Myös ohjelmiston suomenkielisyys on hyödyllinen ominaisuus useimmille käyttäjille. Aloittelevalle tietokoneen käyttäjälle on tärkeää, että ohjeet ja tuki ovat saatavilla. Tietoturvapaketin tulisikin olla sellainen, että se huomioisi niin edistyneet käyttäjät kuin vasta-alkajat. (Kaartinen, 84–90.)

12.3 Ilmaisia tietoturvaohjelmia

Kaupallisten tietoturvaohjelmien lisäksi on Internetissä tarjolla runsaasti ilmaista tietoturvaa tarjoavia sovelluksia. Näiden sovellusten tietoturvataso ei vastaa kaupallisia sovelluksia, mutta ne tarjoavat perussuojaa. Kokeneet käyttäjät saattavat pärjätä ilmaisillakin tietoturvaohjelmistoilla, mutta aloittelijoille niitä ei voi suositella, sillä ne ovat vaikeaselkoisempia, kuin kaupalliset sovellukset. Lisäksi näiden sovellusten päivityksiä ei tule yhtä usein, mikä merkitsee heikentynyttä suojaa. (Yläjääski & Antson, 24–32.)

Ilmaista virustorjuntaa tarjoavat esimerkiksi Antivir Personal Edition ja Alwil Avast! Home edition. Ilmaisia palomuureja on myös tarjolla Sunbelt Kerio Personal Firewall ja ZoneAlarm tarjoavat ilmaisen palomuurin. ZoneAlarmin ilmaispalomuuri päihittää jopa monet kaupalliset palomuurit. Mainos- ja vakoiluohjelmien etsimiseen on kotikäyttäjälle useita ilmaisia työkaluohjelmia. Näiden ohjelmien parhaimmistoa ovat Lavasoftin AD-Aware SE, Spybot – Search & destroy, sekä uusi Microsoft Defender. Mainos- ja vakoiluohjelmien torjujien etuna on, että niitä voidaan asentaa tietokoneelle useita yhtä aikaa. Tietoturvaa voidaankin lisätä esimerkiksi asentamalla kaupallinen tietoturvaohjelman rinnalle yksi tai useampia ilmainen mainos- ja vakoiluohjelmien torjuja. (Yläjääski & Antson, 24–32.)

Useiden kaupallisten tietoturvaohjelmien valmistajien sivulta löytyy selainperustaisia virustarkastussovelluksia. Jos virustartuntaa on syytä epäillä, voidaan näin tietokone tarkistaa. Selainpohjainen tarkistus ei korvaa kuitenkaan oikeaa torjuntaohjelmaa sillä jatkuva suojaus ei sillä onnistu. (Yläjääski & Antson, 24–32.)

13 MARKKINOILLA OLEVIA TIETOTURVAPAKETTEJA JA NIIDEN VERTAILU

Tietoturvaohjelmat näyttelevät suurta roolia tietokoneen turvaamisessa. Erilaisia kaupallisia tietoturvaohjelmia on suuri määrä ja onkin tärkeää ymmärtää minkälaisia ominaisuuksia ohjelmat sisältävät. Jokainen vertailtavista tietoturvaohjelmistoista sisältää perustorjuntaan kuuluvat palomuurin sekä virustorjunnan. Tietoturvapaketeista jokaisen voi laskea luotettavaksi ratkaisuksi henkilökohtaisen tietoturvan takaamiseen. Erot tulevatkin lähinnä lisäominaisuuksien määrästä ja laadusta sekä käyttöliittymien käyttömukavuuksien eroista. Omaan kotikoneeseen kannattaakin valita sellainen ohjelmisto, jonka lisäominaisuuksia kokee itse tarvitsevansa. (Kaartinen, 84–90.)

13.1 F-secure Internet Security 2006

Kotimainen F-secure Internet Security 2006 on koti- että yrityskäyttöön soveltuva tietoturvapaketti. F-Secure on täysin suomenkielinen, sekä ohjeita että tukea on saatavilla suomeksi. Ohjelmassa on erinomainen käyttöliittymä sekä monipuoliset ominaisuudet. Selkeä hallintakonsoli näyttää ohjelmiston tilan havainnollisesti ja luotettavasti yhdellä silmäyksellä. Myös palomuurin ilmoitukset ovat selkeitä. F-securen käyttöönotto on miellyttävä ja sen päivitykset toimivat ripeästi. Edistyneille käyttäjille on tarjolla monipuoliset säädöt, joilla ei kuitenkaan häiritä vasta-alkajia. Kannettavaa tietokonetta käyttävät käyttäjät on huomioitu säädöillä, joiden avulla turvataso voidaan asettaa sopivaksi ympäristön mukaan. (Yläjääski & Antson, 24–32.)

F-Secure sisältää varsin kattavat lisäominaisuudet perinteisten virustorjunnan sekä palomuurin lisäksi. Se sisältää sähköpostin tarkistuksen viruksista sekä roskapostisuodatuksen. Vakoiluohjelmien suojaus on toteutettu käytönaikaisena aktiivisuojauksena. Vakoiluohjelmia on mahdollista etsiä myös manuaalisella etsinnällä. F-securen erikoisuus on piiloutuvien rootkit-ohjelmien torjunta Blacklight-tekniikalla. F-secure onkin ainoa tunnettu tietoturvapaketti, joka sisältää rootkit-ohjelmien torjunnan. Ohjelmisto sisältää lisäksi lapsia varten suunnitellun Websisällönsuodattimen sekä lapsilukon, jolla voidaan kontrolloida lasten Internetin käyttöä aikarajoituksilla. (Yläjääski & Antson, 24–32.)

F-Securen valtti on sen tarjoaman tietoturvan taso. Ohjelmiston turvatarkastukset ovat tiukat ja kansainvälisissä tutkimuksissa torjunnan taso on saanut kiitosta. Haittaohjelman havaitsemisen jälkeen haittatunnistepäivitykset ovat käyttäjien työasemilla kuuden tunnin sisällä, joka on erinomainen päivitysaika. Tietoturvan taso näkyy kuitenkin suurena tietokoneen muistinkulutuksena. F-Secure on raskas ohjelmisto. Tiedostojen manuaalinen tarkistus on myös hidas. (Kotilainen, 66–68.) F-secure Internet Security 2006 valittiin sekä MikroPc:n, että Mikrobitin tietoturvaohjelmisto vertailujen voittajaksi.

F-securea tarjotaan useiden palvelutarjoajien, kuten Elisan, Soneran ja PHP:n laajakaistaliittymien mukana kuukausihintaan. Palvelu maksaa 4-8 euroa kuussa. Useimmiten palveluntarjoajalta hankittu palvelu sisältää lisäksi ilmaisen puhelintuen tietoturvaan liittyvissä ongelmatilanteissa. F-securen voi hankkia myös pakettina kaupasta, jolloin sen hinta on noin 80 euroa. Ohjelmiston osto tarkoittaa vuoden käyttölisenssiä, jonka ajan ohjelmistoon saa päivityksiä. F-securen lisenssiin voi saada vuoden jatkoajan noin 55 euron hintaan. (Yläjääski & Antson, 24–32.)

13.2 Symantec Norton Internet Security 2006

Symantec Norton Internet Security 2006 on suomenkielinen toimivan käyttöliittymän omaava ohjelmisto. Norton antaa asennuksesta lähtien viimeistellyn ja laadukkaan kuvan tietoturvapaketistaan. Ohjelmisto on sopiva sekä kuluttaja- että yrityskäyttöön. Nortonin hallintakonsoli on selkeä ja helposti hallittava kokonaisuus vaikkakaan ei aivan F-securen veroinen. Tietoa tarjoavat lokit ovat erinomaisesti toteutettu. Nortonin palomuurin viestit ovat erittäin havainnollisia. Norton sisältää automaattisen ohjelmistojen tunnistuksen, jonka avulla palomuuri osaa päästää luotettavat ohjelmat ulkoverkkoon ilman häiritseviä kyselyjä. Ohjelmiston selkeät ohjeet helpottavat ohjelmiston käyttöä. Ohjelmisto sisältää mahdollisuuden erilaisiin tietoturvaprofiileihin. Tämä palvelee etenkin liikkuvaa käyttäjää. (Yläjääski & Antson, 24–32.)

Norton sisältää todella paljon lisäominaisuuksia. Sähköpostitarkastus sekä roskapostin esto on toteutettu esimerkillisesti. Vakoilu- sekä mainosohjelmien torjunta kuuluvat ohjelmistoon. Web-sivustojen suodatukseen Norton sisältää sekä lapsille sopimattomien sivustojen tarkistuksen, että tehokkaan mainoksien suodattimen. Luottokortin numeroita ja muita tietoja vakoilevia hyökkäyksiä vastaan ohjelmisto sisältää niin sanotun Antiphishing ominaisuuden. Antiphishing ominaisuus on henkilökohtaisten tietojen suojausohjelma, jolle kerrotaan lista tiedoista ja tunnuksista, joita verkkoon ei saa lähettää. Jos ohjelmaan listattuja tietoja yritetään lähettää verkkoon, ohjelma estää tämän toimenpiteen. (Yläjääski & Antson, 24–32.)

Nortonin vahvuus on helppokäyttöisyys. Se huomio varsinkin aloittelevat tietokoneen käyttäjät. Norton asentaa Windows Xp:n tietoturvakeskuksen tilalle oman paremman versionsa, jonka avulla mahdolliset tietoturvanpuutteet korjataan yhdellä napinpainalluksella. Kuten F-Secure on myös Norton tietokoneen raskas ja resursseja kuluttava ohjelmisto. (Kotilainen, 66–68.)

Symantec Norton Internet Security 2006 maksaa noin 80 euroa. Päivityksien jatkovuosi on hinnaltaan noin 45 euroa. Päivityksen seuraavaan versioon saa 60 eurolla. Nortonia myydään useiden tietokonepakettien lisänä, jolloin vuoden päivityslisenssi on ilmainen. (Yläjääski & Antson, 24–32.)

13.3 Panda Platinium 2006 Internet Security

Panda Platinium 2006 Internet Security on toimiva tietoturvaohjelmisto, jonka käyttöliittymässä on hieman parantamisen varaa. Erilaisia tasoja on turhan paljon, mikä tekee kokonaisuuden hahmottamisen hieman sekavaksi. Panda on kokonaan suomenkielinen. Ohjelmiston käyttöönotto ei suju ongelmitta, sillä sen päivityksien käyttöönotto vaatii kömpelön oloisen rekisteröitymisen. Palomuurin ilmoitukset ovat melko selkeitä, mutta sovelluksen asetusten hallinta voisi olla monipuolisempi. Kuten Norton, sisältää Panda kannettavaa käyttävää helpottavat ohjelmiston asetusprofiilit. Virustarkistus on nopea, mutta sen raportit ovat pelkistettyjä. (Yläjääski & Antson, 24–32.)

Lisäominaisuuksina Pandassa on sähköpostin haittaohjelmatarkistus sekä roskapostisuodatus, joka on toimiva, mutta säätömahdollisuuksiltaan suppea. Myös vakoilu- ja mainosohjelmien torjunta on Pandassa tuettu. Web-suodatusta tarjotaan lapsille sopimattomien sivujen estolla. Ohjelmisto sisältää perustason Antiphishing ominaisuuden. Lisäksi Panda osaa varoittaa uusista langattomaan lähiverkkoon kytkeytyvistä laitteista. (Yläjääski & Antson, 24–32.)

Panda on asennuksen jälkeen erittäin helppokäyttöinen ohjelmisto, sillä se on lähes läpinäkyvä. Ohjelmiston toimintaa tuskin huomaa käytössä. Panda huolehtii toiminnastaan kiitettävästi, eikä sen asetuksista tarvitse usein huolehtia. Lisäarvona Panda sisältää vapaata suoritintehoa tarkastelevan virusajastuksen. (Kaartinen, 84–90.)

Panda Platinium 2006 Internet Security tietoturvapaketti on hinnaltaan muita vertailtavia ohjelmia edullisempi ja maksaa noin 65 euroa. Panda tarjoaa lisäksi vuoden mittaista oikeutta päivityksiin. Jatkopäivitykset ovat hinnaltaan 50 euroa, jolla saa myös mahdolliset ohjelmistopäivitykset. (Yläjääski & Antson, 24–32.)

13.4 McAfee Internet Security Suite 2006

McAfee Internet Security Suite 2006 on varsin kattava tietoturvapaketti, mutta kokonaisuudessa on puutteita. McAfee ohjelmistosta ei ole suomenkielistä versiota saatavilla lainkaan. Ohjelmiston hallintakonsoli on siisti, mutta päälle liimatun tuntuinen. Tietoturvapaketin jokaisella osalla on omat erilliset tilaruutunsa. Tästä syystä asetukset on jaettu turhan moniin erillisiin ruutuihin ja yleiskuvan saaminen on vaivalloista. Asennuksen jälkeen on päivitysten hakeminen käynnistettävä erikseen ja käyttäjälle vaivalloisia tietokoneen uudelleenkäynnistyksiä vaaditaan usein päivitysten yhteydessä. Virustorjunnan asetukset ovat puutteelliset, sillä esimerkiksi tarkistuksista ei voida rajata pois yksittäisiä kohteita. Haittaohjelman tarkistus on lisäksi hidas suorittaa. Palomuurin asetukset ovat monipuoliset, mutta käyttöliittymä ei ole tarpeeksi selkeä käyttää. (Yläjääski & Antson, 24–32.)

McAfee:n lisäominaisuudet ovat hyvällä tasolla. Ohjelmisto sisältää sähköpostien haittaohjelmatarkistuksen sekä erittäin hyvän roskapostisuodatuksen. Vakoilu- ja mainosohjelmien poistoa tarjotaan sekä käytönaikaisena aktiivitorjuntana että manuaalisina tarkistuksina. Internetin käyttäjille ohjelmisto tarjoaa sekä lapsille sopimattomien sivujen suodatuksen että mainoksien suodatuksen. McAfee sisältää myös Antiphishing ominaisuuden. (Yläjääski & Antson, 24–32.)

McAfeen paras ominaisuus on sen monipuoliset säätömahdollisuudet. Varsinkin tietokoneen tehokäyttäjille, joita tietoturva kiinnostaa, on ohjelmisto suositeltava vaihtoehto, sillä ohjelmisto tekee monipuoliset lokit ja tilastot kaikesta tietokoneella tapahtuvasta tietoturvaan liittyvästä toiminnasta. (Kaartinen, 84–90.)

McAfee Internet Security Suite 2006 tietoturvapaketti on noin 80 euron hintainen. Ohjelmiston osto takaa päivitysoikeuden vuodeksi. Vuoden mittaisen päivitys jatkoajan saa noin 60 euron hintaan. (Yläjääski & Antson, 24–32.)

14 CASE: F-SECURE INTERNET SECURITY 2006 TIETOTURVARATKAISUN TESTAUS

Tietoturvapaketteja verratessa tuli nopeasti selväksi, että verrattavista ohjelmistoista F-Secure Internet Security 2006 on tällä hetkellä kotikäyttöön sopivin tietoturvaratkaisu. Ylivoimaisten tietoturvaominaisuuksiensa lisäksi sen lisäominaisuudet ovat erittäin kattavat, kuten taulukkoa 1 tarkastelemalla selviää. Ainoastaan Antiphishing sekä mainostensuodatus lisäominaisuuksien puute voidaan laskea tietoturvapakettia heikentäväksi tekijäksi. Tärkeää on että aloittelevat käyttäjät on huomioitu. Tarjotun ohjeistuksen ja tuen määrä on erinomaisella tasolla. Palveluntarjoajalta ostettuna palveluna on F-Secure myös hinnaltaan ehdottomasti edullisin vaihtoehto.

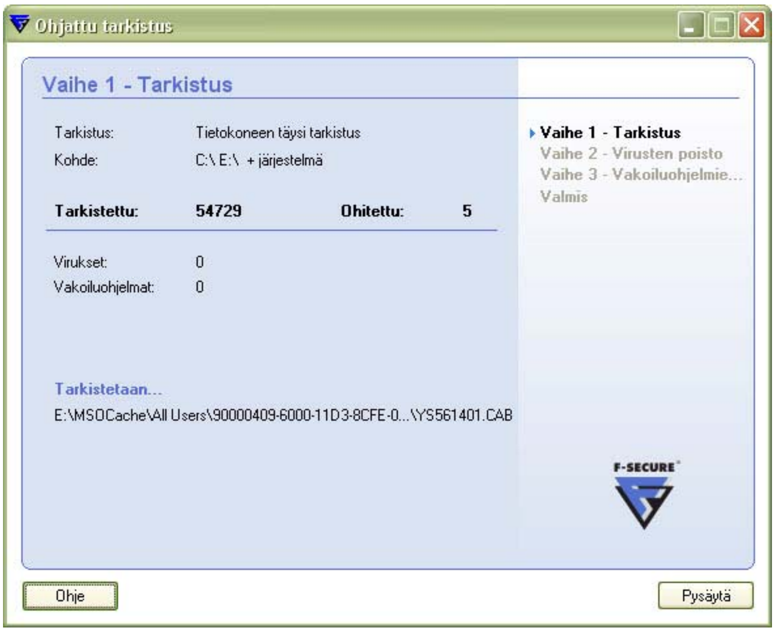
TAULUKKO 1. Tietoturvaohjelmien ominaisuudet (mukailtu lähteestä: Yläjääski & Antson, 26–27)

Ominaisuudet	F-Secure Internet Security 2006	Symantec Norton Internet Security 2006	Panda Platinum 2006 Internet Security	McAfee Internet Security Suite 2006
Suomenkielinen	on	on	on	ei
Sähköpostin tarkistus	on	on	on	on
Roskapostisuodatus	on	on	on	on
Käytönaikainen mainos ja vakoiluohjelmien suodatus	on	on	on	on
Manuaalinen mainos ja vakoiluohjelmien suodatus	on	on	on	on
Rootkit-torjunta	on	ei	ei	ei
Web-mainos suodatin	ei	on	ei	on
Lapsille sopimattomien sivujen esto	on	on	on	on
Lasten Internet käyttöajan valvonta	on	ei	ei	ei
Antiphishing ominaisuus	ei	on	on	on
Wlan seuranta	ei	ei	on	ei
Hinta	80€, päivitys 55€, palveluntarjoajalta 4-8€	80€, päivitys 45€, päivitys seur. ohjelma	65€, päivitys seuraavaan ohjelma	80€, päivitys 60€

14.1 Asennus ja käyttöönotto

F-Secure Internet Security 2006 ohjelmiston asennus on vaivaton ja yksinkertainen. Ohjelmiston saa käyttövalmiiksi varsin nopeasti. Asennus kysyy alussa vaadittavat lisenssiavaimet ja kansion, johon ohjelma asennetaan. Asennuksen jälkeen ohjelma vaatii tietokoneen uudelleenkäynnistyksen.

Tietokoneen käynnistyttyä ohjelma päivittää automaattisesti virustietokantansa ja avaa ohjatun aloitus toimintaruudun. Toimintaruudussa on selkeät ohjeet F-Securen käyttöönottoon. Ensimmäisenä valitaan käytettävä Internetselain ja sähköpostiohjelma. Ohjelma tarjoaa myös mahdollisuuden ottaa roskapostin suodatus ominaisuudet käyttöön. Tämän jälkeen lapsien suojeluasetukset voidaan ottaa käyttöön. Seuraavaksi valitaan tehtävät, jotka halutaan seuraavaksi suorittaa. Tarjolla on täysi manuaalinen virustarkistus, viikoittaisen virustarkistuksen käyttöönotto, ja pääkäyttöliittymän avaus. Valintojen jälkeen alkaa täysi virustarkistus tarkastaa tiedostoja. Täysi tarkastus suoritetaan kolmessa vaiheessa. Ensin tarkastetaan, ettei tiedostoissa ole viruksia, jonka jälkeen suoritetaan niiden mahdollinen poisto. Kolmannessa vaiheessa tarkastetaan, ettei kiintolevyllä esiinny vakoiluohjelmia ja suoritetaan poisto, jos poistettavaa löytyy (KUVIO 2). Tarkistus kestää suhteellisen kauan ja sen aikana on huomattavissa järjestelmän selkeää hidastumista.



KUVIO 2. Täysi tarkistus (F-Secure Internet Security 2006)

Kun tietokonetta aletaan käyttää normaalisti, yrittävät muutamat sovellukset ottaa yhteyttä verkkoon ja F-Securen palomuuri kysyy yhteydenottoikkunan avulla halutaanko näitä sovelluksia päästää verkkoon. Suuri osa sovelluksista, kuten käyttöjärjestelmän käyttämät palvelut, saavat verkkoon yhteyden F-securen määritysten avulla automaattisesti. Yhteydenpyyntöikkunat, eli porttien avaaminen palomuuriin, jotta sovellukset voivat liikennöidä ulkoverkossa, ovat selkeitä ja havainnollisia. Ongelmallista on kuitenkin, että mistä käyttäjä tietää mitkä yhteyspyyntöä yrittävistä ohjelmista on turvallista päästää ulkoverkkoon (KUVIO 3).

KUVIO 3. Uudet yhteysyritykset (F-Secure Internet Security 2006)

14.2 Ohjelman käyttökokemukset

Asennuksen jälkeen on F-secure Internet Security 2006 todella helppokäyttöinen. Kolmen viikon testiajanjakson aikana ei sen toimintaan ollut tarvetta puuttua kertaakaan. Ohjelmisto tarjoaakin lähes näkymätöntä suojaa. Vaikka ohjelmistoa onkin sanottu raskaaksi, ei käytössä ollut tietokone hidastunut sen käytöstä lainkaan. Ongelmia ohjelmiston käytössä ei esiintynyt.

F-Securen hallinta on helppoa hallintakonsolin avulla (KUVIO 4). Kaikki tarpeellinen tieto ohjelmiston tilasta löytyy pääsivulta. Ohjelmiston lisäominaisuuksien perusasetuksia hallitaan välilehdillä. Välilehdiltä voi asetuksia muuttaa yksinkertaisesti. Välilehdillä on kohta lisäasetukset, josta voidaan muokata yksityiskohtaisesti ohjelmiston eri asetuksia. Käytännössä asetuksia ei tarvitse monestikaan muuttaa vaan oletusarvoisilla asetuksilla selviää erinomaisesti. Asetuksien muuttaminen on kuitenkin helppoa selkeän käyttöliittymän ansiosta.

KUVIO 4. Selkeä käyttöliittymä (F-Secure Internet Security 2006)

14.2.1 Välilehdet ja ominaisuudet

F-Securen käyttöliittymä koostuu useista välilehdistä. Jokainen välilehti sisältää jonkin ominaisuuden tai osa-alueen tietoturvapaketin toiminnasta. Välilehtien ansiosta kaikki tarpeellinen tieto löytyy helposti ja asetukset saadaan muutettua muutamalla napin painalluksella. Päävälilehtiä on kuusi: pääsivu, virus- ja vakoilusuojaus, Internet suojaus, roskapostin hallinta, lapsilukko ja automaattiset päivitykset. Jako on selkeä, joten käyttäjälle ei jää epäselväksi minkä välilehden alta mikäkin ominaisuus löytyy.

Pääsivu välilehti kertoo yleiskuvan ohjelmiston nykyisestä tilasta ja asetuksista. Pääsivun avulla on helppoa muokata ohjelmiston kaikkia perusasetuksia. Pääsivulta löytyy myös tietoturvauutisia tietoturvasta kiinnostuneille käyttäjille. Nämä uutiset kertovat lähinnä uusista leviävistä haittaohjelmista.

Virus ja vakoilusuojaus välilehdeltä voidaan ajaa manuaaliset haittaohjelma tarkistukset ja määrittää käytönaikaisen suojauksen asetuksia. Välilehti tarjoaa myös mahdollisuuden muuttaa virus- ja vakoilusuojauksen tasoa tehokkaammaksi tarpeen mukaan.

Internet suojaus välilehdeltä muutetaan palomuurin asetuksia. Tästä voidaan esimerkiksi säätää tiukempia palomuuriasetuksia, kun tietokonetta käytetään esimerkiksi Internet-kahvilan verkossa. Välilehdeltä voidaan myös muokata palomuuriasetuksia sovelluskohtaisesti ja sulkea esimerkiksi aiemmin avattuja portteja.

Roskapostin hallinta välilehdeltä hallitaan roskapostin torjunta asetuksia. Ohjelmisto suojaa roskapostilta monia yleisimpiä sähköpostiohjelmia, kuten Microsoft Outlook, Microsoft Outlook Express, Opera, Netscape, Mozilla Thunderbird ja Eudora, mutta ei Internetin kautta toimivia web-sähköposteja. Testityöasemalle luotiin sähköpostiosoite, jota käytettiin Mozilla Thunderbird sähköpostiohjelmalla. F-securen ohjeiden avulla oli roskapostisuodatusten käyttöönotto suhteellisen helppoa. Sähköpostiosoitetta jaettiin mainostajien listoille epämääräisiin Internet osoitteisiin, jotta osoitteeseen saataisiin roskapostia. Roskapostia alkoikin tulla ja se päätyi poikkeuksetta roskapostikansioon. Voidaankin todeta, että roskapostin suodatus oli käytössä tehokas.

Lapsilukkovälilehti sisältää asetukset lapsien suojelemiseen Internetin vaaroilta, sekä mahdollisuuden kontrolloida perheen pienimpien Internetin käyttöä ajastuksella. Kun lapsilukko otetaan käyttöön, asetetaan salasana, jotta asetuksia ei voida muuttaa ilman lupaa. Suodatettavat Internet sivut voidaan valita eri kategorioista, kuten uhkapeli, aikuisviihde, aseet ja Chat. Suodatus vaikutti tehokkaalta sillä esimerkiksi Chat suodatuksen ollessa päällä, esti ohjelmisto pääsyn Chatin sisältäville sivuille varsin tehokkaasti. Suodatuksien lisäksi lapsilukkovälilehti sisältää ominaisuuden, jolla voidaan rajata Internetin käyttöä. Tämä tapahtuu asettamalla aikalukkoon kellonajat, jolloin Internetin käyttö on sallittua. Muina aikoina ei Internetiä voi käyttää. Aikalukko osoittautui testikäytössä erinomaiseksi, sillä sen asettamia Internetin käyttörajoituksia ei pystynyt kiertämään edes muuttamalla Windows Xp:n kellonaikaa.

Automaattiset päivitykset -välilehti sisältää tiedot ohjelmiston saamista päivityksistä. Tietoja ovat esimerkiksi milloin virustunnisteet on viimeksi päivitetty ja milloin web-suodatus on viimeksi päivitetty. Välilehti sisältää myös tarkasta nyt -napin, jonka avulla ohjelmisto tarkistaa onko uusia päivityksiä saatavilla. Jokaista välilehteä on selkeä käyttää ja tarvittavat asetukset löytyvät nopeasti. Tarvittaessa näkyviin saa lisäksi suomenkielisen ohjesivun, jolla kerrotaan selkeästi miten ohjelmistoa käytetään.

14.3 Johtopäätökset

Kokonaisuutena F-Secure lunastaa sille asetetut odotukset. Ohjelmiston käyttöönotto on erittäin helppoa selkeiden ohjeiden ja hiotun käyttöliittymän ansiosta. Asennuksen jälkeen ohjelmisto on täysin käyttövalmis. Vaikka käytönaikana ei haittaohjelmia, kuten viruksia havaittu, tuntee ohjelmaa käyttäessä tietoturvan olevan turvattu. Ohjelmisto on tietokonetta käyttäessä lähes näkymätön, eikä se häiritse turhilla kyselyillä. Poikkeuksena ovat eri ohjelmien yhteydenpyyntö ikkunat palomuurin läpi, joista asiaan perehtymättömän on mahdotonta päätellä onko ohjelma hyödyllinen vai haitallinen.

Ohjelman käyttöliittymä on erinomainen ja selkeä. Lisäominaisuudet, kuten lapsilukko sekä vakoiluohjelmientorjunta, on toteutettu helppokäyttöisiksi ja tehokkaiksi. F-Secure sisältää selkeät ohjeet ja tukea saa myös puhelimitse. Ohjelmisto sopii niin aloittelevalle kuin kokeneille käyttäjälle helppokäyttöisyyden, erinomaisen tietoturvan ja monipuolisten ominaisuuksien ansiosta. Ohjelmistoa on helppoa suositella kaikille hyvää tietoturvapakettia tarvitseville.

15 YHTEENVETO

Tietokoneen turvaaminen on pitkä ja monivaiheinen, jatkuvaa ylläpitoa vaativa prosessi. Tärkeä osa työaseman suojausta ovat tietoturvaohjelmat. Ilmaisten tietoturvaohjelmien turva ei ole vielä yhtä hyvä hitaampien päivitysten ja vaikeamman hallinnan vuoksi, joten on viisainta valita kaupallinen tietoturvapaketti. Tietoturvaohjelmien kaupalliset versiot ovat erittäin hiotut. Tietoturvapaketit, jotka ovat nykyisin erittäin helppokäyttöisiä ja kattavia. Nähtävissä on kehitys, jonka edetessä ei tietoturvapaketin toimintaan tarvitse enää asennuksen jälkeen puuttua ollenkaan. Nykyiset tietoturvapaketit tarjoavat erinomaista suojaa työasemalle. Käyttäjän on kuitenkin huolehdittava, että ohjelmisto saa tietoturvapäivitykset säännöllisin väliajoin.

Pelkkä tietoturvaohjelma ei kuitenkaan yksinään riitä suojaamaan tietokonetta, vaan monista muistakin asioista tulee huolehtia. On tärkeää muistaa ettei tietoturva ole tuote, jonka voi ostaa kaupasta tai asentaa valmiista paketista. Absoluuttista tietoturvaa ei ole olemassa, sillä paraskaan tietoturvaohjelmisto ei pysty täysin turvaamaan käyttäjän tietokonetta. Tietoturvaan on opittava. Käyttäjää tuleekin ohjeistaa tietokoneen oikeaoppiseen käyttöön ja siihen kuinka tietokone tulee suojata. Liian usein unohdetaan esimerkiksi kuinka tärkeää on suojata ja varmuuskopioida tärkeät tiedostot. Tietoturvallisen ympäristön aikaansaamiseksi tulee käyttäjän oppia tietynlainen vainoharhainen asenne. Kaikkeen tulee pyrkiä varautumaan etukäteen, kuten varmuuskopioimalla tiedostot. Tärkeää on myös tietää, kuinka ongelmatilanteissa tulee toimia. Vaikka tietoturvaohjelmat ovat erittäin tärkeä osa tietokoneen turvaamista, vastaa viime kädessä tietoturvantasosta kuitenkin käyttäjä itse.

15.1 Tutkimuksen tavoitteiden toteutuminen

Tässä tutkimuksessa perehdyttiin tietoturvaan ja siihen liittyviin tekijöihin. Tietoturva on aiheena kiinnostava sekä ajankohtainen. Tutkimukseen perehtyminen oli helppoa, sillä tietoturva oli minulle jo ennestään tuttu aihe. Opinnäytetyö ei opettanut minulle paljoakaan uusia asioita vaan lähinnä vahvisti jo aiemmin opittuja näkemyksiä tietoturvasta. Uutta oli kuitenkin esimerkiksi se, kuinka tärkeä osa tietokoneen suojaamista varmuuskopiointi on. Mielestäni tutkimus antaa hyvän yleiskuvan kotitietokoneen tietoturvaan liittyvistä vaaroista ja suojauskeinoista. Esimerkiksi tietoturvaohjelmia käsitellään opinnäytetyössä laajasti. Työssä esitetyn tietoturvavertailun avulla on helppoa aloittaa itselle sopivimman tietoturvaohjelman valinta. Allekirjoittanut on harkinnut vakavasti F-Secure Internet Security 2006 täyslisenssin ostoa. Kokonaisuutena työ vastaa mielestäni sille asetettuihin odotuksiin.

LÄHTEET

Kirjalliset lähteet

Järvinen, P 2002. Tietoturva & yksityisyys. Docendo Finland Oy. WS Bookwell, Porvoo.

Boström, M 2003. Kotimikron tietoturva. Talentum media Oy. Gummerus kirjapaino Oy, Jyväskylä.

Hakala, Vainio, Vuorinen 2006. Tietoturvallisuuden käsikirja. Docendo Finland Oy. WS Bookwell, Porvoo.

Ruohonen, M 2002. Tietoturva. Docendo Finland Oy. WS Bookwell, Porvoo.

Hakkerin käsikirja, 2002. IT Press. Edita Prima Oy, Helsinki.

Symantec, Sulje ikkunasi kutsumattomilta vierailta. Tietoturvaa pienyrityksille. 2004. Kristianstads Boktryckeri AB.

Ylä-Jääski, V & Antson, J. Turvaa pakettiin. MikroPC 2/2006, 24–32.

Verkkohyökkäys kotona. Mikrobitti 11/2006, 9-10.

Kaartinen, S. Turvallisuuden tunne. Mikrobitti 01/2006, 84–90.

Kotilainen, S. Tietoturvapaketit paisuvat. Tietokone 02/2006, 66–68.

Elektroniset lähteet

F-Secure Internet Security 2006 Opetusohjelma [verkkodokumentti], 2006 [viitattu 20.10.2006]. Saatavissa: http://support.f-secure.fi/enu/home/elearning/is2006el_fin/start.htm

Kansalaisen mikrotuki [verkkodokumentti], 2006 [viitattu 10.8.2006]. Saatavissa: http://www.kansalaisenmikrotuki.fi

Wikipedia Roskaposti [verkkodokumentti], 2006 [viitattu 11.8.2006]. Saatavissa: http://fi.wikipedia.org/wiki/Roskaposti

Tietoturvaopas tietoturvaohjelma [verkkodokumentti], 2006 [viitattu 2.12.2006]. Saatavissa: http://www.tietoturvaopas.fi/fi/index.html

F-Securen tietoturvakatsaus heinä-joulukuu 2006: hiljaisuus voi olla petollista [verkkodokumentti], 2006 [viitattu 6.12.2006]. Saatavissa: http://www.f-secure.fi/2006/2/