Tiina Lehtonen

TIETOTURVA JA TIETOTURVAOHJELMISTOT

Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto
2011

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

TIETOTURVA JA TIETOTURVAOHJELMISTOT

Lehtonen, Tiina
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Toukokuu 2011
Ylikoski, Mauri
Sivumäärä: 45

Asiasanat: tietoturva, turvallisuus, virustorjuntaohjelmat

Tämän opinnäytetyön aiheena oli tutkia tietoturvaa sekä tietoturvaohjelmistoja. Opinnäytetyötä aloittaessa tutkittiin tietoturvaan liittyviä artikkeleita ja näiden artikkeleiden perusteella luotiin opinnäytetyölle runko ja se, kuinka laajasti asioista lähdetään kertomaan. Opinnäytetyössä tutkittiin myös kahden suositun tietoturvaohjelman ominaisuuksia ja vertailtiin näitä.

Teoriaosuudessa perehdyttiin tietoturvan peruselementteihin eli virus- ja haittaohjelmiin. Tietoturvan velvollisuuksissa ja oikeuksissa kerrottiin teleyrityksen velvollisuuksista, sekä henkilörekisterin ja yhteisötilaajan tarkoituksesta. WLAN-verkon turvallisuuteen liittyvässä osiossa kerrottiin uhista ja verkon suojaamisesta. Opinnäytetyön teoriaosuudessa kerrottiin myös hieman erilaisten maksullisten ja ilmaisten tietoturvaohjelmien perusteista.

Käytännön osuudessa tutkittiin kahden tunnetun tietoturvaohjelmiston asetuksia, tehtäviä, toimintojen eroavaisuuksia sekä ominaisuuksia. Opinnäytetyön vertailtaviksi tietoturvaohjelmistoiksi valittiin kaupallinen F-Secure Client Security ja ei-kaupallinen Avast! Antivirus -ohjelma.

Tietoturvan päivittäminen, siitä huolta pitäminen ja tietoturvaohjelman asentaminen omalle koneelle on suositeltavaa. Ei pidä sokeasti luottaa omaan tietoturvaohjelmaan. Vaikkakin tietoturvaohjelman viruspäivityksien pitäisi aina olla ajan tasalla, voi yhtäkkiä tulla jokin uusi virus tai haittaohjelma, jota ei ole vielä tunnistettu ja tällöin viruspäivityksetkään eivät asennu. Suosittelisin ennemmin Avastin asentamista peruskäyttäjän tietokoneelle sen helppokäyttöisyyden takia, F-Securen ohjelma sopii paremmin ammattilaisen/yrityksen käyttöön.

DATA SECURITY AND DATA SECURITY SOFTWARE

Lehtonen, Tiina
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information Technology
May 2011
Ylikoski, Mauri
Number of pages: 45

Key words: Data security, security, antivirus software

The subject of this thesis was to research data security and security software. When starting this thesis security related articles were explored. Based on these items the thesis body was created and it was thought that, how far to go to tell these things. This thesis also examined two popular security softwares features which were then compared.

In the theory part, basic security elements, antivirus- and malware programs were explored. In security rights and responsibilities the company's obligations and also person registers and corporate subscribers purpose were located. In the WLAN security related section it explained about the threats and network protection as well. In the thesis theory section it was also mentioned about different paying and free security programs.

In the practical part two well-known security software's settings, tasks, function differences and features were explored. In this thesis the compared security software were; commercial F-Secure Client Security and non-commercial Avast! Antivirus program.

Updating security, taking care of it and installing security software on your computer is recommendable. You should not blindly trust your own security program. Although the security program's antivirus updates should always be up to date, may there suddenly come some new virus or malware, which has not yet been identified, then the antivirus updates will not be installed. I recommend installing Avast on a home user's computer, because it is easy to use. F-Secures program is better suited for professional/business use.

SISÄLLYS

LYHENTEET JA TERMIT

FreeBSD	Vapaa Unix-käyttöjärjestelmä. FreeBSD on keskittynyt suorituskykyyn.
IM	Tarkoittaa pikaviestintää (Instant Messaging). Pikaviestinnällä tarkoitetaan tietoverkon välityksellä tapahtuvaa viestinvaihtoa. Pikaviestiohjelmia ovat mm. Skype ja Windows Live Messenger.
OpenBSD	Unixin kaltainen vapaa käyttöjärjestelmä. OpenBSD:n tärkein painotus on turvallisuudessa.
Palomuurisääntö	Tämän avulla voidaan ohjata palomuurin käyttäytymistä sekä sallia tai estää haluttua liikennettä.
P2P	Vertaisverkko (peer to peer). Verkko, jossa jokainen verkossa oleva taho toimii palvelimena ja asiakkaana verkon muille jäsenille.
Rootkit	Ohjelmisto, joka asentuu tietokoneelle, kun hyökkääjä saa koneen haltuunsa. Rootkit-ohjelmat voivat esim. muokata tietokoneen käyttöjärjestelmää ja korvata perustoimintoja.
SSID	Langattoman lähiverkon tunnus (Service Set Identifier). SSID:n avulla voidaan erottaa ne WLAN-verkot toisistaan, jotka ovat samalla alueella ja voidaan kytkeytyä haluttuun verkkoon.

WEP	Työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaaman kehitetty salausmenetelmä. Tarkoituksena on suojata langatonta verkkoa salakuuntelulta ja estää luvattomilta käyttäjiltä pääsy verkkoon. WEP-salaus on purettavissa helposti kotikonstein, joten se on lähes hyödytön salausmenetelmä.
WPA	Tietoturvatekniikka, joka kehitettiin WEP-salauksen ongelmien paljastuttua (Wi-Fi Protected Access). WPA käyttää salauksessa dynaamista avainta, joten avain muuttuu jatkuvasti ja tämän takia verkkoon murtautuminen on vaikeampaan kuin WEP-salauksessa.

1 JOHDANTO

Pidä tietoturvastasi huolta! Nykypäivänä tietoturva koskee jokaista tietokoneen omistajaa. Yksityisten ihmisten ja yrityksen tehtävänä on ylläpitää hyvää tietoturvatasoa, vaikka tietokoneella ei olisikaan mitään varastettavan arvoista. Tietoturvan ollessa huono, voi tietokoneeseen tapahtua hyökkäyksiä verkon ulkopuolelta ja tällöin voi tulla tietokoneeseen mittavaa tuhoa.

Tietoturvaohjelmien tarkoituksena on poistaa viruksia ja haittaohjelmia sekä estää niiden toimintaa. Tietoturvaohjelman on hyvä olla käyttäjän kannalta helppokäyttöinen ja, että ohjelman tekemät tehtävät ovat automaattisia. On kuitenkin mahdollista, että vaikka pitäisitkin hyvää huolta tietoturvastasi, niin koneellesi voi silti päästä jostain syystä jokin virus- tai haittaohjelma.

Päätin tehdä opinnäytetyöni itseäni kiinnostavasta aiheesta, jonka lisää tietämisestä voisi olla hyötyä tulevaisuudessakin. Tahdon pitää huolen siitä, että oman tietokoneeni tietoturva-asiat ovat kunnossa.

Opinnäytetyöni tarkoituksena on kertoa tärkeimpiä asioita tietoturvasta, virus- ja haittaohjelmilta suojautumisesta sekä erilaisista tietoturvaohjelmista. Opinnäytetyössäni käytännön osuudessa tutustuin melko tarkasti kahden tunnetun virustorjuntaohjelman toimintaan. Opinnäytetyöni pitää sisällään myös tietoturvan perusasioiden kertomista. Opinnäytetyöni tavoitteena on tutustuttaa lukija tietoturvan perusasioihin.

2 TIETOTURVA

Tietoturvan tarkoituksena on tietojen, palveluiden, järjestelmien sekä tietoliikenteen suojaaminen. Uhkina tietoturvalle ovat muun muassa piratismi, henkilökohtaisen yksityisyyden loukkaus, roskaposti sekä tietokonevirukset.

2.1 Mitä on tietoturva

Internetin tietoturvasta puhuttaessa tarkoitetaan sillä usein kaikkea Internet-liikenteen turvallisuuteen liittyviä asioita. Tietoturvalla tarkoitetaan sitä, että koneella käsiteltyihin tietoihin eivät pääse käsiksi ne tahot, joilla ei ole oikeuksia annettu niiden käsittelyyn. Yksityisyyden kannalta tietoturva on turvallista tietojenkäsittelyä. Arkaluontoista tietoa hankkivaa ei-toivottua henkilöä sanotaan hakkeriksi, hakkeri suorittaa tietomurtoja saadakseen tietoja haltuunsa.

Tietoturvalle asetettuja tavoitteita:

- Yksilön tai organisaation annettujen tietojen luottamuksellisuus
- Eheys eli oikeellisuus (integrity): Tarkoittaa tiedon muuttumattomuutta tiedon luomisen, käsittelyn ja siirron aikana.
- Kiistämättömyys: Valvotaan tiedonsiirtoon tai käsittelyyn osallistuneiden käyttäjien tunnistamista. Tämä varmistaa sen, että tietoja ei voi käsitellä huomaamatta.
- Pääsynvalvonta: Valvotaan ja rajoitetaan käyttäjien tietoihin käsiksi pääsyä.
- Saatavuus: Tarkoitetaan sitä, että oikeuksien haltijoilla on helppo ja viiveetön käyttö.
- Tarkastettavuus: Tarkoitetaan sitä, että pitää kyetä tarkastamaan tietojenkäsittelyn tuloksena saatu tieto ja kyettävä osoittamaan sen oikeellisuus.

Jotta tiedot pysyvät luottamuksellisina, pitää niiden olla vain niihin oikeutettujen käytössä. Tietojen ja dokumenttien turvaluokitus määrittelee sen, että kenellä on tietojen ja dokumenttien käyttö-, säilytys- ja tuhoamisoikeus.

2.1.1 Tietoturva Internetissä

Tietoturva on keskeinen kysymys Internetissä. Verkkoympäristön kautta voi mm. Muunnella luvatta WWW-sivustojen tietoja, internet-hakuja voi ohjata vääriin osoitteisiin, sähköpostia voi lähettää väärillä nimillä ja toisten käyttäjien käyttäjätunnuksia ja salasanoja voi kaivaa esiin sekä myös luottokorttien numeroita. Huonosti toteutetun tietoturvan seurauksia voivat olla virukset tai se, että ulkopuoliset henkilöt tunkeutuvat tietojärjestelmiin. Jos ulkopuolinen henkilö tunkeutuu tietojärjestelmään, voi tämän seurauksena olla tietojärjestelmien sisältämien tietojen väärinkäytökset tai ilkivaltaiset tuhoamiset. /1/

2.2 Virukset ja haittaohjelmat

Virukset ja madot ovat pieniä tietokoneohjelmia, jotka toimivat haittaohjelmina. Nämä ohjelmat leviävät koneesta toiseen Internetin, sähköpostin tai tiedostojen välityksellä. Niiden toimintaa ei käyttäjä edes aina huomaa. Virukset jaetaan makro- ja käynnistyslohkoviruksiin.

Käyttäjän tietojen hävittäminen on suurin vahinko, jonka virukset tietokoneelle päästyään voivat tehdä. Virus voi tyhjentää kiintolevyn tilavaraustaulukon. Informaatio ei tällöin ole fyysisesti kadonnut vaan tiedostot voidaan palauttaa itse jollain apuohjelmalla tai kovalevyn voi toimittaa tehtävään erikoistuneeseen liikkeeseen. Virus voi myös toimia tuhoisammin täysin näkymättömissä, tällöin se kirjoittaa kiintolevylle roskakoodia. Viruksen havaitseminen on tuolloin vaikeaa ja tuhotkin voivat olla suuria, koska varmuuskopiotkin ovat saastuneita. Ylikirjoitettuja tietoja ei enää saa myöskään palautettua. Virukset voivat myös sotkea tietokoneen muistin aiheuttaen käyttöjärjestelmän toimintaan häiriöitä.

Suurin osa viruksista sisältää vain leviämiseen tarkoitetun ohjelman, eikä tee tuhoa tietokoneelle. Mahdollista on, että ne aiheuttavat yhteensopivuusongelmia. Tästä voi aiheutua tietokoneen toiminnan hidastumista, tiedostojen tuhoutumista tai henkilökohtaista aineistoa voi levitä Internetiin.

Viruksen toiminta koostuu yhdestä tai kahdesta vaiheesta. Virus levittää itsestään ainoastaan kopiota ensimmäisessä vaiheessa. Viruksen aktivoituminen ja tuho tapahtuu mahdollisessa toisessa vaiheessa. Joissakin viruksissa on vain leviämisosa ja toiset virukset aktivoituvat leviämisen yhteydessä. Osa viruksista odottaa tietyn ajan ennen leviämistä tai aktivoitumista. Tietokone voi muuttua myös roskapostin lähettäjäksi, tällöin tietokone lähettää käyttäjän huomaamatta suuria määriä viestejä. /2/

2.2.1 Viruksilta suojautuminen

Ennaltaehkäisy on ehdottomasti paras keino suojautua virusten haitallisuudelta. Viruksen on mahdotonta aiheuttaa vahinkoa, jos se saadaan tuhottua ennen sen pääsemistä koneeseen. Virustorjunnan uhka pienenee, kun käyttäjä on aktiivinen. Jos virus pääsee varotoimista huolimatta suojauksen läpi, pitää viruksista aiheutuvat vahingot minimoida.

Tietokoneen käyttäjän pitää huomioida ainakin nämä asiat:

- Että tietokoneessa on virustorjuntaohjelmista, jonka virustietokanta päivitetään aina uuden ollessa tarjolla
- Virustorjuntaohjelmiston taustasuojauksen pitää olla aktiivisena
- Palomuurin pitää olla asennettuna ja aktiivisena
- Tuntemattomia tai epäilyttäviä tiedostoja/ohjelmia ei saa asentaa tai käyttää
- Sähköpostin liitetiedoston turvallisuus ja luotettavuus pitää varmistaa
- Lähettäessäsi liitetiedostoja, on hyvä ilmoittaa liitteen sisältö ja ohjelma, jolla se aukeaa.
- Tietokoneen käynnistyksen yhteydessä ei pidä pitää CD-asemassa levyä, jollet ole varma, että se ei sisällä haitallisia ohjelmistoja.
- Varmuuskopioiden ottaminen säännöllisesti /3/

2.2.2 Virusten poistaminen

Kunnon virustorjuntaohjelma poistaa kaikki sen tuntemat virukset automaattisesti. Virusten tuhoamiseen voidaan myös tarvita erillisiä tietoturvayhtiöiden kotisivuilta saatavia korjausohjelmia. Jos koneessa on havaittu virus, tulee se sammuttaa

virtakytkimestä. Jotkut virukset voivat levitä tai aktivoitua koneen uudelleen käynnistyksen yhteydessä. Tarkista ensin, ettei Internet-yhteyttä ole. Ota varmuuskopiot tärkeistä tiedostoista, jos se on mahdollista. Virustorjuntaohjelma valitsee yleensä parhaan vaihtoehdon tilanteen korjaamiseksi automaattisesti. Kiintolevyn täydellinen alustaminen on ainut keino viruksen poistamiseen, jos virustorjuntaohjelma ei pysty poistamaan virusta koneelta.

2.2.3 Phishing-hyökkäyksiltä suojautuminen

Phishingillä tarkoitetaan taloudellisen tiedon, mm. verkkopankkitunnusten, luottokorttinumeroiden sekä henkilötietojen laitonta hankkimista. Tyypillisesti käyttäjän sähköpostiin lähetetyllä viestillä houkutellaan käyttäjää siirtymään jonnekin sivustolle, jossa pitää luovuttaa taloudellista tietoa. Huijaussähköpostiviestit naamioidaan usein näyttämään esimerkiksi rahoituslaitoksen asiakaspalveluviesteiltä.

Sivustot, joissa pyydetään luovuttamaan tietoja voivat näyttää ulkoisesti esimerkiksi rahoituslaitoksen sivuilta. Todellisuudessa tällaisille sivuille syötetyt tiedot päätyvät hyökkääjän käsiin, phishing-hyökkääjä on ottanut haltuunsa tietojärjestelmään luomiaan huijaussivustoja.

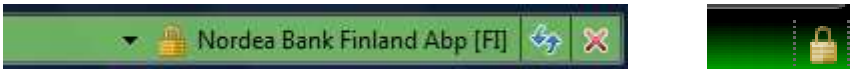
Seuraavassa ohjeessa on ohjeita ainoastaan huijaustapauksiin:

- Rahoituslaitokset (kuten Nordea) eivät kysele koskaan asiakkailtaan sähköpostitse verkkopankkitunnuksia, luottokorttinumeroita tai muuta luottamuksellista tietoa.
- Älä luota sähköpostin lähettäjäkentässä (FROM-kenttä) olevaan sisältöön. Lähettäjäkentän tiedon voi helposti väärentää vaikkapa muotoon asiakaspalvelu@pankki.fi.
- Älä luota siihen, että www-sivustojen tai sähköpostien linkit johtavat sinne, mitä linkeissä lukee.

Suojautuminen:

- Älä avaa epäilyttäviä sähköpostiviestejä. Otsikkotiedoistakin voi jo tunnistaa epäilyttävän viestin.

- Älä siirry koskaan sähköpostilinkin kautta verkkopankin tms. sivustolle. Suhtaudu myös www-sivuilla oleviin linkkeihin suurella varauksella. Turvallisin tapa siirtyä sähköiseen palveluun on kirjoittamalla itse www-sivuston osoite selaimen osoiteriville tai käyttämällä esim. kirjanmerkkiä (bookmark).
- Tarkista aina luottamuksellisia tietoja syöttäessä, että olet oikean organisaation sivustolla ja, että sivustolla on käytössä SSL-suojaus (suositellaan käytettäväksi mm. käyttäjien kirjautumisessa sekä verkkokaupassa) Suojattu yhteys internetpalvelun osoiterivillä alkaa kirjainsarjalla https://. Ja/tai selaimen alareunassa tilarivillä tai osoitekentässä pitää näkyä kiinni oleva lukko. Internet Explorer:



Kuva 1 Internet Explorer (8) osoitekenttä (oik.) sekä Mozilla Firefox (3.5.3)-selaimen tilarivi (vas.)

  Yhteys ei ole suojattu, jos internetosoite alkaa http://. Osoiterivillä olevan osoitteen pitää muodostua pankin verkkotunnuksesta eli domain-nimestä (esim. www.nordea.fi).
- Jos selainohjelma antaa varoituksen, ettei palvelimen varmenne täsmää sivuston osoitteen kanssa suhtaudu riittävällä vakavuudella tilanteeseen.
- Ota yhteys epäilyttävässä tapauksessa organisaation, jonka sähköisestä palvelusta on kyse. /4/

2.2.4 Haittaohjelmilta suojautuminen

Tietojärjestelmien käyttäjillä ja niiden ylläpitäjillä on haasteellinen tehtävä suojautua viruksilta, Troijan hevosilta sekä madoilta. Haittaohjelmilta suojautumisessa pitää seurata jatkuvasti haittaohjelmatilannetta sekä annettuja varoituksia. Tarvittaessa on reagoitava tilanteen asettamiin haasteisiin.

Tämän esimerkinomaisen listan avulla voi varautua ja suojautua haittaohjelmia vastaan:

- Asenna sovellusohjelmistoihin ja käyttöjärjestelmään ajantasaiset päivitykset.
- Asenna virustorjuntaohjelmisto ja päivitä sitä.

- Käytä käyttöjärjestelmäsi palomuuria tai asenna palomuuriohjelmisto, joka vaikeuttaa haittaohjelmien toimintaa.
- Älä asenna koneellesi tuntemattomia tai epäilyttäviä tiedostoja tai ohjelmia.
- Poista epäilyttävät sähköpostiviestit lukematta niitä. Varmista sähköpostin liitetiedoston turvallisuus.
- Älä pidä koneen levykeasemassa levykettä käynnistyksen yhteydessä, jos et ole varma, että se ei sisällä haittaohjelmia.
- Tietojärjestelmästä tulee ottaa varmuuskopio säännöllisesti. /5/

2.3 Tietoturvaohjelmat

Tietoturvaohjelmaa valitessa tärkein toivottu ominaisuus ohjelmalla on tietenkin se, että sillä on kyky suojata tietokonetta viruksilta ja haittaohjelmilta. Ohjelman on hyvä olla helppokäyttöinen ja sellainen, että se mm. hakee uusia viruspäivityksiä automaattisesti. Vanhempien tietokoneiden käyttäjät toivovat, että ohjelman käyttäminen ei vaikuta suuresti suorituskykyyn.

Perinteisiin työasemiin tarkoitetuilla tietoturvaohjelmistoilla on kaksi toimintatilaa: Staattinen tiedostojen tarkastustila ja dynaaminen reaaliaikainen tila. Staattinen tiedostojen tarkastustila on käyttökelpoinen tarkastettaessa, onko levykkeellä tai kovalevyllä saastuneita tiedostoja. Dynaaminen reaaliaikainen tila tarkastaa tiedostot ennen niiden suoritusta, joten tämä tila estää tiedostojen saastumisen.

Tietoturvaohjelmisto saadaan säädettyä toimimaan eri tavoin sen löytäessä saastuneen tiedoston. Mahdollisia toimintatapoja ovat tiedoston karanteeniin asettaminen ja tiedoston puhdistus.

Virustorjunta on siirtynyt osaksi verkkopalveluita haittaohjelmien yleistyttyä. Virustorjuntaohjelmistoja käytetään erityisesti sähköpostipalvelimissa, tiedostopalvelimissa ja www-välityspalvelimissa, joiden tehtävänä on vastaanottaa liikennettä ulkoverkosta tai käyttäjien työasemilta. Sähköpostiliikenteessä poistetaan vastaanottavalla palvelimella haittaohjelmia sisältävät sähköpostiviestit. Tällä estetään se, että virukset tai haittaohjelmat eivät pääse kohdekoneelle aiheuttamaan vahinkoa.

Uusia haittaohjelmia ilmestyy kymmeniä, jopa satoja joka kuukausi. Virustietokantojen säännöllinen päivittäminen on tärkeää, jotta torjuntaohjelma tuntisi ja suojaisi konetta uusilta viruksilta ja haittaohjelmilta. Uusia tartuntoja aiheuttavat sähköpostin mukana leviävät virukset ovat lähes kaikki havaittu viime vuoden aikana ensimmäisen kerran. /6/

Seuraavissa kappaleissa on kerrottu hieman yleisimmistä ilmaisista sekä maksullisista tietoturvaohjelmista.

2.3.1 Ilmaiset tietoturvaohjelmat

2.3.1.1 Avast! Home Edition

Avast! on ilmainen, suosittu virustorjuntaohjelma. Ohjelmasta on olemassa myös maksullinen versio Avast! Professional, joka tarjoaa kattavamman ominaisuuspaketin. Avast! on tsekkiläisen AVAST softwaren kehittämä virustorjuntaohjelma Windows- ja Linux-käyttöjärjestelmille. Ohjelmasta on saatavilla myös suomenkielinen versio. Avast! Home Editionin lisenssi on voimassa aina vuoden. Ohjelmasta lisää vielä myöhemmin. /7/

2.3.1.2 Avira AntiVir

Ohjelmasta on olemassa ilmainen ja maksullinen versio. Ilmainen versio on AntiVir Personal Edition Classic, maksullinen versio (sisältää enemmän ominaisuuksia) on AntiVir Personal Edition Premium. Lisäksi on myös yrityskäyttöön tarkoitettu maksullinen tuoteperhe. Ohjelma on saksalaisen Avira GmbH:n valmistama virustorjuntaohjelma. Avira AntiVir on saatavilla useimmille Microsoft Windowseille, Linux-, OpenBSD-, FreeBSD- sekä Solaris-käyttöjärjestelmille. /8/

2.3.1.3 AVG Anti-Virus

AVG on tsekkiläisen AVG Technologiesin valmistama virus- ja haittaohjelmien torjuntaohjelmisto. Ohjelman maksuton versio on yksityiskäyttöön tarkoitettu AVG Free, jossa on vähemmän ominaisuuksia, kuin maksullisessa versiossa. Ohjelma on englanninkielinen. AVG soveltuu erityisen hyvin vanhoille koneille sen kevyen muistin- ja suoritinkäyttönsä takia. Ohjelma on helppokäyttöinen. /9/

2.3.2 Maksulliset tietoturvaohjelmat

2.3.2.1 F-Secure

Kyseessä on maksullinen suomalaisen yrityksen valmistama ohjelma. F-Securen uusimmat virustorjuntaohjelmistot ovat F-Secure Internet Security 2011 sekä F-Secure Client Security 9 (ohjelmasta myöhemmin lisää). F-Securen tutkimuspäällikkö Mikko Hyppönen esiintyy usein julkisuudessa, kun tietoturvauhkia uutisoidaan. Virustorjuntaohjelmia löytyy kotikäyttöön ja yrityksille. Ohjelma sisältää virustorjunnan, palomuurin, roskapostin suodatuksen, lapsilukon, vakoiluohjelmien tunnistajan. Saatavilla on myös F-Secure Anti-Virus ohjelma, joka on pelkkä virustorjuntaohjelma. Ohjelmistoa eteenpäin myyvät esim. Elisa ja Sonera, jotka ovat brändänneet tuotteen itselleen ja myyvät sitä nimillä Elisa Tietoturvapalvelu ja Sonera Tietoturva –nimillä. /10/

2.3.2.2 Norton Antivirus

Ohjelma on maksullinen Symantec Corporationin valmistama virustorjuntaohjelma. Symantecin päämaja sijaitsee Piilaaksossa, Kaliforniassa. Norton Antiviruksen ensiversio julkaistiin 1990. Vaikkakin ohjelma on laajassa käytössä ympäri maailmaa, on sillä maine hitaana ohjelmana. 2004 versiosta alkaen ohjelma on täytynyt aktivoida Internetissä. Norton on noussut viime vuosina maksullisten Anti-Virusten kärkikastiin. /11/

2.3.2.3 McAfee Antivirus

McAfee on maksullinen Yhdysvaltalainen virustorjuntaohjelma. McAfeen pääkonttori sijaitsee Santa Clarassa, Kaliforniassa. McAfeen tuotteisiin kuuluu mm. McAfee VirusScan sekä McAfee Internet Security. Ohjelma pitää sisällään SiteAdvisor –toiminnan, joka pitää kirjaa Internet-sivustojen turvallisuudesta. Olen kokeillut käyttää ohjelmaa joskus ja todennut, että ohjelma on jopa liian turvallinen, jos näin nyt voi sanoa. Vastaani tuli useita kertoja Internet-selaimella sellainen ”hidaste”, että ohjelma kysyi, onko sivu jolle olet menossa turvallinen ja tällöin piti antaa lupa, että voi edetä sivustolle. Tämä hidasti sivustojen selaamista. /12/

2.3.2.4 Panda Internet Security

Panda on maksullinen Espanjalainen virustorjuntaohjelma. Ohjelma suojaa viruksilta, vakoiluohjelmilta, rootkiteiltä, hakkereilta, verkkohuijauksilta, identiteettivarkauksilta ja muilta tunnetuilta ja tuntemattomilta uhilta. Ohjelmassa on mukana lapsilukko-ominaisuus, jonka avulla lapsi voi selata Internetiä turvallisesti. Panda Securityn (www.pandasecurity.com) sivuilta voi tarkistaa oman tietokoneen Active Scan-onlinen avulla viruksia, haittaohjelmia ja muita Internetin uhkia vastaan. /13/

2.4 Yksityishenkilön tietoturva

Yrityksille tietoturva on suuri asia, mutta myös yksittäisen Internetin käyttäjän pitää myös suhtautua varauksella Internetin tietoturvaan. Tietojen varastajat tietävät, että yksittäisellä ihmisellä voi myös on olla yhtä tärkeää tietoa koneillaan kuin yritysten julkisilla tietokoneilla.

Yksityisen henkilön tietokoneella voi olla tietoa, jota yksityishenkilö ei ole tarkoittanut muiden käsiin kuten työtehtäviin liittyviä dokumentteja, tunnuksia ja salasanoja työkoneille, tilinumeroita, luottamuksellista ja salaista tietoa

Yksityishenkilön tietoturvan pitää olla kunnossa, jottei koneen tietoihin pääse käsiksi ulkopuolinen henkilö, joka tarkoituksella etsii juuri arkaluontoisia tietoja koneelta. Yksityishenkilön pitää ymmärtää myös, että voi olla ulkopuolisia tietoturvariskejä ns. inhimillisiä tekijöitä. Tällainen voi olla esimerkiksi se, että henkilö antaa salasanan ja käyttäjätunnuksen ulkopuoliselle henkilölle. Jos yksityisen henkilön tietokone on suojattu näillä tunnuksilla, ulkopuolinen henkilö pääsee käsiksi tietoihin. Tällöin tietoturvaa on taas rikottu. /14/

2.5 Yrityksen tietoturva

Yritykselle tärkeät tiedot pyritään suojaamaan tietoturvalla. Tämän tarkoituksena on taata yhtiön tietojen koskemattomuus. Tietoturvan tarkoitus yritykselle on se, että liiketoiminnan tarpeita tuetaan sekä sisäiset ja ulkoiset vaatimukset täytetään. Perinteisesti tietoturvallisuudella tarkoitetaan eheyden, luottamuksellisuuden ja käytettävyyden turvaamista.

Tietoturva tarjoaa tietosuojan ylläpitämiseen erilaisia keinoja ja toimintamalleja, rakennetaan ikään kuin muuri suojattavan tiedon ympärille. Tietoturvan kannalta on olennaista tietää tietosuojaa koskevat perusasiat.

Tietoturvallisuus on pieniä tekoja osana jokapäiväistä toimintaa. Jokaisen pitää ymmärtää tietoturvallisuuden merkitys ja työskennellä sen saavuttamiseksi ja ylläpitämiseksi. Tietoturvallisuus tulee suunnitella huolella, toteuttaa lainsäädännön vaatimukset ja rajoitukset huomioon ottaen ja joiden vaikutuksia tulee seurata toiminnan kehittämiseksi. Hyvän tietoturvallisuustason saavuttaminen ja ylläpitäminen vaatii yritykseltä määrätietoista ja –muotoista toimintaa ja johtamista. Tietoturva tulisi nähdä kilpailuetuna, eikä välttämättömänä pahana, jolla vain kiusataan työntekijöitä. Edellyttäen, että tietoturva on hoidettu asianmukaisesti liiketoiminnan asettamalla tavalla. /15/

3 TIETOTURVALLISUUTEEN LIITTYVÄT VELVOLLISUUDET JA OIKEUDET

Suomessa ei ole varsinaista tietoturvallisuuslainsäädäntöä. Eri laissa ja asetuksissa on sisällytetty tietoturvallisuuden säännökset. Henkilötietojen käsittelyyn ja luottamukselliseen viestinnän suojaan löytyy erilaisia säännöksiä lukuisista eri laista. Sähköisen viestinnän tietosuojalain noudattamisen valvonta kuuluu Viestintävirastolle. Tietosuojavaltuutetun tehtäväksi on säädetty osa valvontatehtävistä.

Viestintäviraston valvoma Viestintämarkkinalaki sisältää teleyrityksiä koskevan yleisen tason tietoturvallisuusvelvoitteen. Viestintävirasto valvoo myös säännösten ja määräysten noudattamista sähköisen viestinnän tietosuojalain ja viestintämarkkinalain nojalla. /16/

3.1 Teleyrityksen velvollisuuksista

Teleyrityksen velvollisuutena on huolehtia palvelujensa tietoturvasta. Huolehtiminen tarkoittaa sitä, että tehdään toimenpiteitä toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden suhteen. Toimet tulee suhteuttaa uhkien vakavuuden, teknisen kehitystason sekä kustannusten kesken. Teleyritys on aina vastuussa tarjoamansa palvelun tietoturvallisuudesta, vaikka yritys olisikin ulkoistanut osia palvelustaan.

Teleyrityksen oikeutena on ryhtyä heti toimiin palvelujensa tietoturvan varmistamiseksi tietoturvaloukkausten torjumisen sekä tietoturvahäiriöiden poistamiseksi. Teleyrityksen mahdollisuutena on viestien välittämisen ja vastaanottamisen estäminen, tietoturvaa vaarantavien haittaohjelmien poistaminen viesteistä ja muiden näihin rinnastuvien teknisluonteisten toimenpiteiden toteuttaminen palvelussaan. Toimenpiteisiin ryhtymisen oikeus on vain, jos se on

välttämätöntä turvatakseen verkko- ja viestintäpalvelun. Toimenpiteet pitää toteuttaa rajoittamatta sananvapautta tai luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä. Toimenpiteet lopetetaan heti, kun palvelun tietoturvallisuuden varmistaminen ei niitä enää edellytä.

Erilaiset suojaustoimenpiteet pitää tehdä viestinnän sisältöön puuttumatta, jos tämä vain on mahdollista. Jos näyttää siltä, että viesti voi sisältää järjestelmää vaarantavan haittaohjelman tai, että viestiä käytetään tietoliikenteen häirintään, voi teleyritys tällöin puuttua viestin sisältöön teknisin keinoin viestin tarkastamiseksi ja poistamiseksi.

Teleyrityksen tehtävä on tiedottaa asiakkailleen, että palveluun kohdistunut tietoturvaloukkaus tai –uhka on poistettu. Tiedottaminen ei saa johtaa palvelun tietoturvallisuuden uudelleen vaarantumiseen.

Teleyrityksen yleisenä velvollisuutena on ilmoittaa käyttäjän käytettävissä olevista toimenpiteistä uhkan torjumiseksi sekä näistä aiheutuvista todennäköisistä kustannuksista. Teleyrityksen tehtävänä on ADSL-liittymiä markkinoidessaan kertoa avoimen tietoverkon uhista tilaajalle ja suositella virustorjunta- ja palomuuriohjelmiston käyttämistä.

Teleyrityksen pitää ilmoittaa Viestintävirastolle verkko- ja viestintäpalvelujen merkittävistä tietoturvaloukkauksista ja –uhista. Teleyrityksen pitää ilmoittaa myös, jos palvelussa on merkittäviä vika- ja häiriötilanteita. /17/

3.2 Henkilörekisteri

Henkilörekisterillä tarkoitetaan henkilötietoja sisältäviä tietojoukkoja, jos niitä käsitellään tietojenkäsittelyn avulla tai kyseessä on kortisto, luettelo tms., josta tietyn henkilön tiedot voi löytää helposti ja ilman kohtuuttomia kustannuksia. /18/

Henkilötietojen käsittelyn tarkoitus määritellään siten, että siitä selviää, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään. /19/

Henkilörekisterinpitäjän velvollisuutena on huolehtia henkilötietojen suojaamisesta (henkilötietolaki 32§). Toimenpiteitä toteutettaessa täytyy ottaa huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteistä aiheutuvat kustannukset, käsiteltävän tiedot laatu, määrä ja ikä. On otettava huomioon myös se, että mikä on käsittelyn merkitys yksityisyyden suojan kannalta.

Rekisterinpitäjän puolesta toimivan itsenäisen elinkeinoharjoittajan pitää antaa rekisterinpitäjälle ennen tietojen käsittelyyn ryhtymistä asianmukaiset sitoumukset ja riittävät takeet henkilötietojen suojaamisesta.

3.3 Yhteisötilaaja

Yritykset ja yhteisöt, jotka käsittelevät viestintäverkossaan (sisäisissä puhelin- ja tietoverkoissaan) käyttäjien luottamuksellisia viestejä, tunnistamis- ja paikkatietoja ovat yhteisötilaajia. Yhteisliittymäjärjestelyt taloyhtiön asukkailla voivat myös olla yhteisötilaajia. Vaikka perheellä kotona olisikin sisäinen tietoverkko tai puhelutietoja tallentava laite, perhettä ei kuitenkaan katsota yhteisötilaajaksi. /20/

Yhteisötilaajan velvollisuutena on huolehtia käsittelemiensä tunnistamis- ja paikkatietojen tietoturvallisuudesta.

Yhteisötilaajan oikeus on ryhtyä välttämättömiin toimiin käsittelemiensä tietojen tietoturvan varmistamiseksi, jotta tietoturvaloukkauksia torjuttaisiin ja tietoturvaan kohdistuvia häiriöitä poistettaisiin. Yhteisötilaaja pystyy siis estämään viestien välittämisen ja vastaanottamisen, poistamaan haittaohjelmat, jotka vaarantavat tietoturvaa ja toteuttaa muita viestintäverkon teknisluonteisia toimenpiteitä. Yhteisötilaajalla on oikeus ryhtyä näihin toimenpiteisiin vain välttämättömien verkko- tai viestintäpalvelun tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi. Toimenpiteillä ei saa rajoittaa sananvapautta tai luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä. Toimenpiteet lopetetaan heti, kun palvelun tietoturvallisuuden varmistaminen ei enää edellytä niitä.

Mahdollisuuksien mukaan on tehtävä suodatustoimenpiteet viestinnän sisältöön puuttumatta. Viestit voidaan teknisesti tarkistaa ja suodattaa viestin sisällön perusteella, jos on epäily, että viesti saattaa sisältää haittaohjelman tai viestiä käytetään tietoliikenteen häirintään. /21/

4 LANGATTOMAN LÄHIVERKON (WLAN) TURVALLISUUS

WLAN mahdollistaa tietojärjestelmän kytkeytymisen langattomaan tietoverkkoon. WLAN-verkkoja käytetään monissa julkisissa tiloissa mm. hotelleissa, lentokentillä, kahviloissa ja kouluissa tarjoamalla kannettavien päätelaitteiden käyttäjille pääsy Internetiin. Myös monet yritykset käyttävät WLAN-verkkoja, mutta WLAN-verkkojen käyttö on yleistynyt erityisesti kotikäyttäjien keskuudessa.

Ennen langattoman lähiverkon käyttöönottoa pitää huomioida niin yritys- kuin kotikäytössäkin langattomiin lähiverkkoihin liittyvät riskit. Tavallisimmat WLAN-verkkoihin liittyvät uhat:

- Salaamatonta liikennettä on helppo kuunnella verkon kuuluvuusalueella. Usein langattoman lähiverkon kuuluvuusalue ulottuu laajemmalle alueelle kuin verkkoa suunniteltaessa on otettu huomioon. Yrityksessä käytössä oleva WLAN saattaa olla myös yrityksen toimitilojen ulkopuolella käytettävissä ja kuunneltavissa.
- Langattomat verkot ovat kaikkien verkon kuuluvuusalueella olevien saatavissa ilman tunnistautumista. Tällöin on mahdollista käyttää ulkopuolisen tahon osalta WLAN-verkkoa väärinkäytöksiin, esim. roskapostien levittämiseen.
- Jos organisaation sisäverkko on suoraan kytketty langattomaan lähiverkkoon, voi sisäverkon järjestelmiin tunkeutua langattoman lähiverkon kautta.

WEP-salaus, jota yleisesti käytetään WLAN-verkoissa sisältää heikkouksia, heikkouksien takia se on helposti murrettavissa. Ulkopuolinen voi kuunnella verkon liikennettä ja käyttää verkkoa omiin tarkoituksiin, jos WEP-salaus murretaan (jos verkossa on käytössä yksinomaan WEP-protokollaan pohjautuva tunnistautuminen).

Suojautuminen:

- Käytä liikenteen salaukseen ja tunnistautumiseen vähintään WEP-protokollaa. Uusimmassa WPA2-protokollassa on korjattu useita WEP-protokollan heikkouksia. WPA2-protokollan käyttöä suositellaan, jos laitteet ja ohjelmistot vain tukevat sitä.
- Jos tunnistautumisessa on käytössä salasana, ei salasana saa olla helposti arvattava. Ota myös käyttöön MAC-osoitteisiin pohjautuva tunnistautuminen.
- SSID:n mainostaminen kytketään tukiasemista pois.
- WLAN-verkkoa tulee hallinnoida vain kiinteän kaapelin kautta
- WEP:n tai WPA:n lisäksi riittävän vahva salaus on aina tarpeen, jos WLAN-verkossa siirretään arkaluontoisia tietoja

Laite- ja ohjelmistovalmistajien käyttöohjeissa on edellä mainituista suojausmenetelmien käyttöönotosta yksityiskohtaiset tiedot. WLAN-verkkoja yrityksessä tai yhteisöissä käytettäessä tulee ottaa huomioon seuraavat asiat:

- WLAN-verkkoa ei saa liittää suoraan yrityksen sisäverkkoon. WLAN-verkko on hyvä kytkeä palomuurin ulkopuolelle topologisesti.
- WLAN-verkon turvatasovaatimukset tulee huomioida aina. Ennen kun verkko otetaan käyttöön, pitää WLAN-verkon riskit analysoida erityisen tarkasti ja huolellisesti.
- Pitää huomioida, että WLANin suojaamisella suojataan ainoastaan verkkoyhteyden ”viimeiset metrit” (kaupungissa 10-30 m, maaseudulla 1-15 km). /22/

4.1 SSID

SSID-tunnuksen avulla asiakkaat kytkeytyvät haluamaansa langattoman verkon tukiasemaan eli Access Pointiin (AP). SSID on yleensä saman valmistajan tuotteissa sama, joten se kannattaa muuttaa käyttöönoton yhteydessä, jotta sekaantuminen naapurin verkon kanssa vältetään. Yleensä Access Point-laite voidaan asettaa laittamaan SSID-tietoa ilmatielle, tämä ominaisuus on monessa laitteessa oletuksena päällä. Jos asia on näin, ei asiakkaan tarvitse tietää SSID:tä kytkeytyäkseen verkkoon. Hyötyä tästä on silloin, jos halutaan esimerkiksi yrityksessä tai oppilaitoksessa antaa vierailijoiden käyttää jotain osaa verkosta tai, jos verkko on

tarkoitettu julkiseksi. Jos asiattomien vierailijoiden pääsy verkkoon halutaan estää, tällöin ominaisuus voidaan kytkeä pois käytöstä tai voidaan valita ns. hidden-SSID-toiminto.

4.2 Pääsylistat

Access Point-listalla voidaan rajoittaa ulkopuolisten henkilöiden pääsyä verkkoon. Access Point-listalla määritellään ne asiakaslaitteiden MAC-osoitteet, joilla sallitaan pääsy verkkoon. Huonona puolena tällä on se, että verkon ylläpitäjälle tulee tästä ylimääräistä työkuormaa, koska hänen pitää lisätä jokainen MAC-osoite manuaalisesti jokaisen verkon tukiaseman pääsylistaan. Joillakin tukiasemavalmistajilla on kuitenkin tarjolla ohjelmistoja, joilla listojen hallinta voidaan toteuttaa koostetusti, mutta osoitteet pitää silti lisätä edelleen manuaalisesti.

MAC-osoitelistaa ei tule pitää kovinkaan tehokkaana tapana rajoittamaan verkkoon pääsyä, koska MAC-osoitteet kulkevat selväkielisinä paketeissa, vaikka data olisikin salakirjoitettu. Tunkeutuja voi helposti selvittää jonkin verkossa käytetyn MAC-osoitteen ja muuttaa oman verkkokorttinsa MAC:n vastaamaan tätä. /23/

5 TIETOTURVAOHJELMIEN TESTAUS

5.1 Avast! Free Antivirus

Yhteenveto-valikko

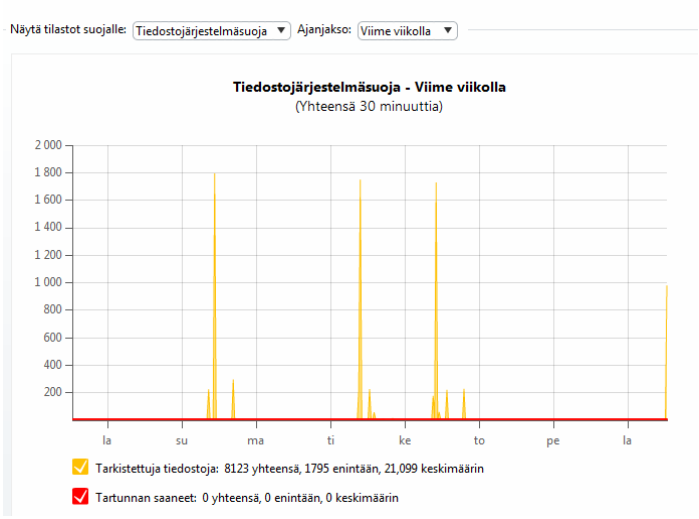
Kuva 2. Avast! yhteenveto-valikko

Valikosta näkee sen, että tietokone on täysin suojattu.

Nykyinen tila

Hiljaisen/pelitilan päällä oleminen tarkoittaa sitä, että onko pelitila on päällä. Jos pelitila on päällä Avast ei toista mitään ääniä tai näytä näytöllä mitään viesti-ikkunoita, mikä häiritsisi pelaamista.

Tilastot



Kuva 3. Avast! tilastot-valikko

Tämän kautta voit tarkastella ohjelmamoduulien tekemiä tilastoja. Moduulin voit valita pudotusvalikosta. Valittavina on: Tiedostojärjestelmäsuoja, sähköpostisuoja, selainsuoja, vertaisverkkosuoja, pikaviestinsuoja, verkkosuoja sekä käyttäytymissuoja (lisää tästä alempana ”tosiaikaisessa suojassa”).

Tarkista tietokone

Kuva 4. Avast! tarkista tietokone -valikko

Valikon kautta voit muuttaa tarkistuksen asetuksia. Voit myös tehdä oman tarkistusluvan.

Tarkista nyt

Tässä tarkistus-asetukset, joita voit muuttaa:

- Pikatarkistus. Tämän avulla teet nopean tarkistuksen tärkeimmille järjestelmätiedostoille ja tietokoneen keskusmuistille.
- Koko tietokoneen tarkistus. Tarkistaa koko tietokoneen. On perusteellinen, mutta myös hitaampi tapa.
- Siirrettävien muistien tarkistus. Jos tietokoneeseen on kytketty mm. muistitikku tai siirrettävä kiintolevy, tarkistaa tämä silloin nämä ulkoiset muistit.
- Valitse tarkistettavat kohteet. Voit valita kohteet, jotka tarkistetaan. Kohteet valitaan ennen tarkistuksen aloittamista.

Tarkistus käynnistyksen alussa

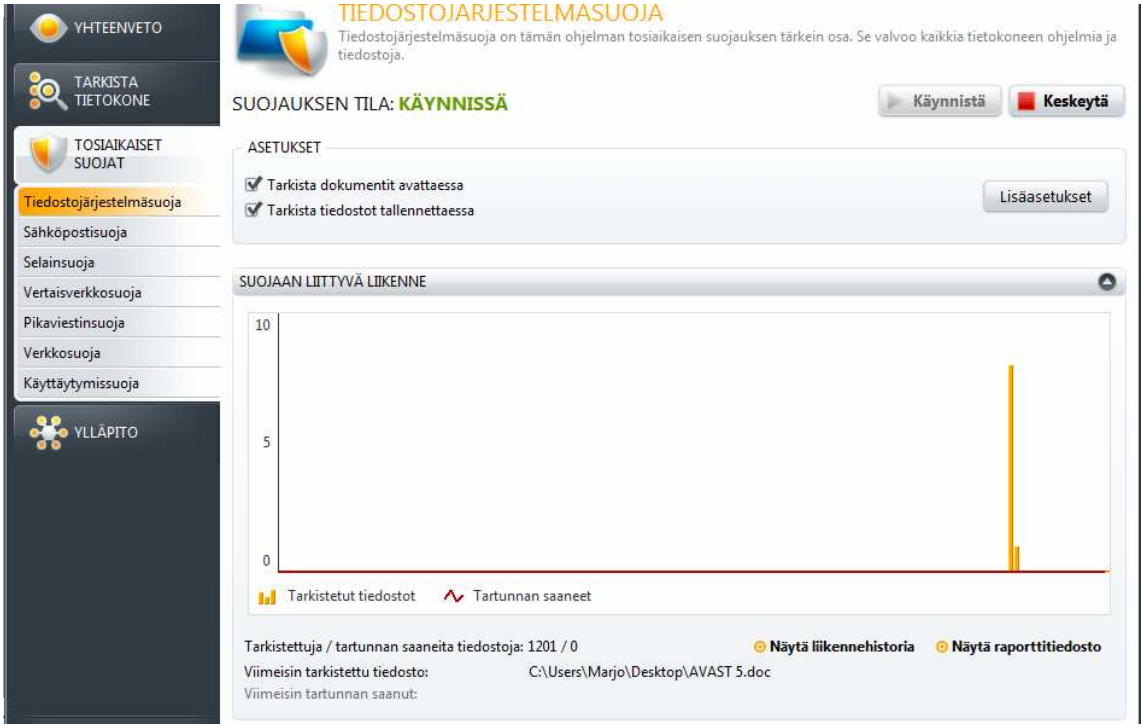
Tietokoneen käynnistyksen alussa tehdään tarkistus ennen Windowsin käynnistämistä. Tämän ansiosta mahdolliset haittaohjelmat eivät käynnisty ja ne voidaan poistaa ennen, kun vahinkoa aiheutuu. Kaikkein vaikeimmin poistettavissa olevat rootkit-ohjelmat löytyvät yleensä alussa suoritettavan tarkistuksen ansiosta.

Valikosta voit valita, otetaanko tarkistus käyttöön vai pois käytöstä. Voit myös valita, mitkä ovat tarkastettavat kohteet eli onko se kaikki tietokoneen kiintolevyt vai järjestelmäasema.

Tarkistusraportit

Taulukosta näet kaikki suoritetut tarkistukset, ajastetut tarkistukset sekä löydetyt tartunnat.

Tosiaikaiset suojat



Kuva 5. Avast! tosiaikaiset suojat-valikko

- Tiedostojärjestelmäsuoja: Tosiaikaisen suojauksen tärkein osa. Valvoo kaikkia tietokoneen ohjelmia ja tiedostoja. Asetuksista saat määriteltyä ne tiedostot ja ohjelmat, jotka tarkistetaan ajettaessa eli tarkistetaanko dokumentit avattaessa ja tiedostot tallennettaessa. Alhaalla liikkuva ”pylpyrä” tai ”pylpyrät” ilmoittavat, kuinka paljon tiedostoja on tarkistettu ja kuinka paljon on tartunnan saaneita tiedostoja. ”Pylpyrät” ovat myös jokaisessa muussa moduulissa käytössä.
- Sähköpostisuoja: Tarkistaa kaikki lähtevät ja saapuvat viestit. Saapuneet viestit tarkistetaan jo ennen, kun ne ovat käytettävissä sähköpostiohjelmassa, joten tartunnan saaneet viestit eivät pääse ainakaan vahingoittamaan tietokonettasi. Asetuksista saat muutettua sähköpostisuojan toimintaa eli tarkistetaanko lähetettävät ja vastaanotettavat viestit sekä uutisryhmien viestit.
- Selainsuoja: Valvoo kaikkea Internet-selaimen ja verkon välillä tapahtuvaa liikennettä. Selainsuoja estää haitallisen ohjelmakoodin pääsyn selainohjelmaan ennen tartuntojen leviämistä. Asetuksista saat muutettua selainsuojan asetuksia: Otetaanko selainsuoja käyttöön ja käytetäänkö älykästä suojaa.
- Vertaisverkkosuoja: Suojaa tietokonetta vertaisverkon kautta leviäviä viruksia vastaan. Vertaisverkkosuojalla ei ole muutettavia perusasetuksia,

mutta voit määritellä mitä vertaisverkko-ohjelmia ohjelmalla voidaan suojata, valittavina on mm. Kazaa, LimeWire, Bit Torrent, uTorrent.

- Pikaviestinsuoja: Suojaa tietokonetta pikaviestiohjelmien kautta leviäviä viruksia vastaan. Tälläkään suojalla ei ole muutettavia perusasetuksia, mutta voit määritellä, mitä pikaviestinohjelmia seurataan, valittavina tässä on mm. MSN Messenger, Yahoo! Messenger, mIRC, Skype, Google Talk.
- Verkkosuoja: Valvoo tietokoneen verkkoliikennettä ja estää niiden virusten toiminnan, jotka verkon välityksellä yrittävät tartuttaa tietokoneen. Asetuksista saa muutettua sen, että näytetäänkö varoitusviestit.
- Käyttäytymissuoja: Tarkkailee tietokoneen toimintaa ja hälyttää, jos epäilyttävää käyttäytymistä havaitaan.

Ylläpito

Kuva 6. Avast! ylläpito-valikko.

Päivitys

Ohjelman toiminnan kannalta on tärkeää, että käytössä on uusimmat päivitykset. Vaikkakin ohjelman oletuksena on automaattisten päivitysten suorittaminen, voit silti muuttaa päivitykseen liittyviä asetuksia.

Voit päivittää tarkistusosan ja virustunnisteet painamalla kohtaa ”päivitä tarkistusosa ja virustunnisteet” ja koko ohjelman saat päivitettyä painamalla ”päivitä koko ohjelma” kohtaa.

Rekisteröinti

Tämän kohdan kautta voit tarkastella rekisteröintiin liittyviä tietoja. Näet myös sen, että koska ohjelma on rekisteröity ja, koska rekisteröinti vanhentuu ja ohjelma pitää rekisteröidä uudelleen.

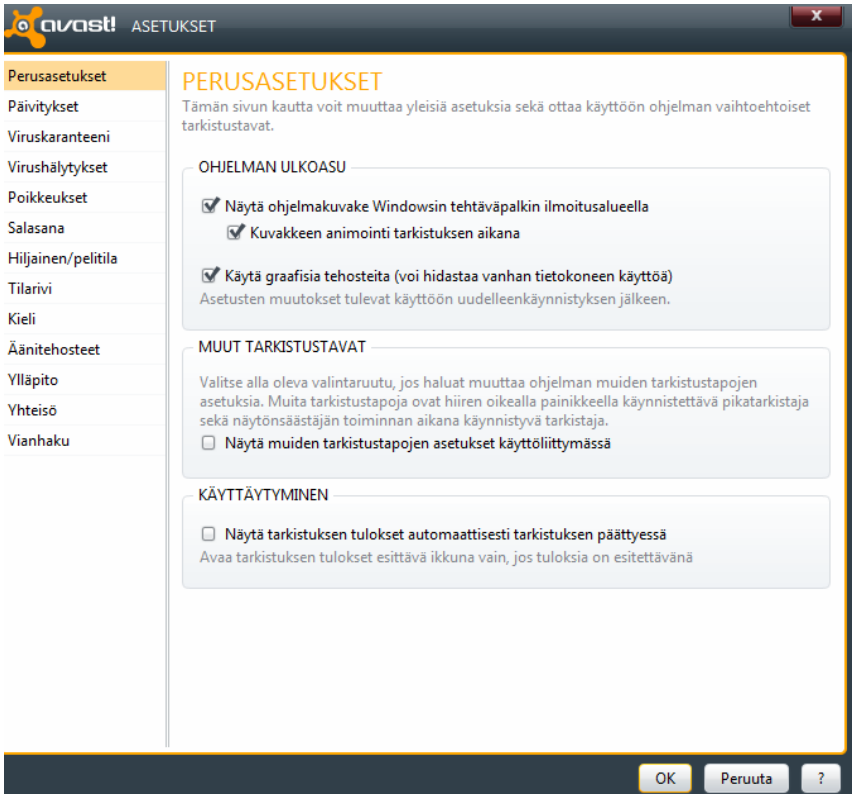
Viruskaranteeni

Tänne varastoidaan epäilyttävät, tartunnan saaneet tiedostot. Kun siirrät tiedoston karanteeniin, voit eristää tiedoston muusta järjestelmästä ja tiedosto ei jatkossa häiritse tietokoneen käyttöä.

Lisätietoja ohjelmasta

Sivulta löytyy ohjelmaan liittyviä yleisiä tietoja. Lisätietoja voit katsoa Internet-sivuilta osoitteesta www.avast.com/about. Internet -sivut ovat englanninkieliset. Lisätietoja ohjelmasta-sivulta näet mm. versionumeron, virustunnisteiden version.

Avast! Asetukset-valikko



Kuva 7. Avast! asetukset-valikko

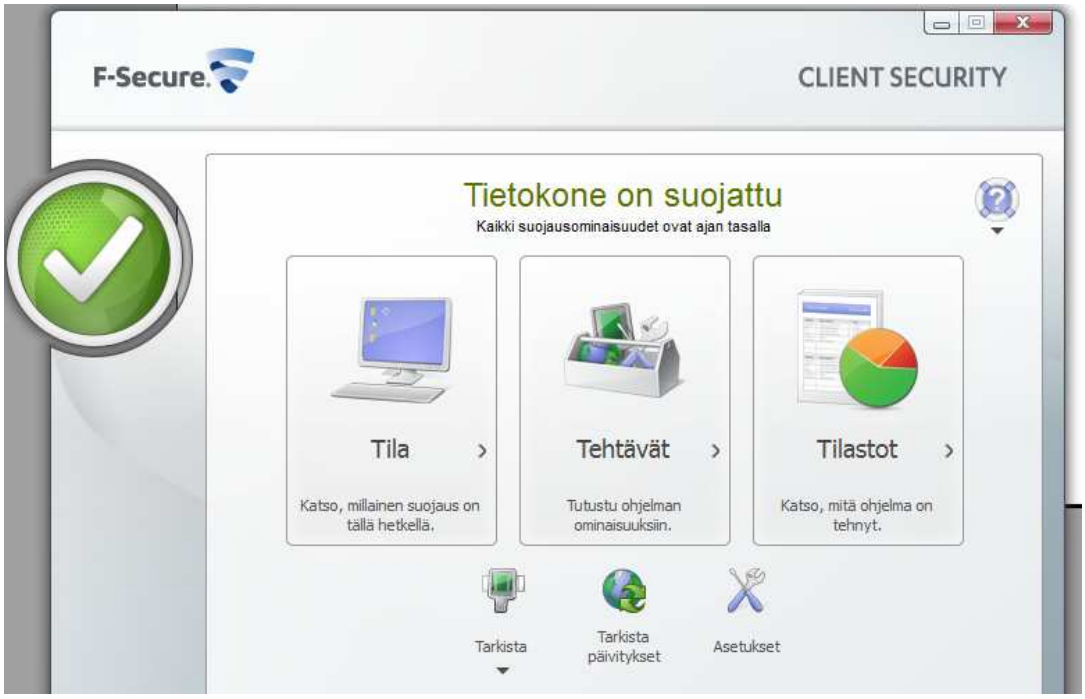
Asetuksien kautta voit muuttaa ohjelman eri asetuksia. Seuraavien asioiden asetuksia voi muuttaa:

- Perusasetukset. Voit muuttaa yleisiä asetuksia, mm. sen, että näkyykö ohjelman kuvake Windowsin tehtäväpalkissa ja käytetäänkö graafisia tehosteita (tämän käyttö voi hidastaa vanhan tietokoneen käyttöä).
- Päivitykset. Voit muuttaa päivitykseen liittyviä asetuksia. Voit valita, että päivitetäänkö viruspäivitys automaattisesti, ehdotetaanko päivityksen tekemistä, kun uusi päivitys on saatavilla vai tehdäänkö päivitys itse. Saat myös määritetyksi sen, että milloin koko ohjelma päivitetään, päivitetäänkö ohjelma automaattisesti silloin kun uusi päivitys on saatavilla, ehdotetaanko uuden päivityksen asentamista vai tehdäänkö päivitys itse.
- Viruskaranteeni. Voit muuttaa viruskaranteenin asetuksia eli sitä, mikä on karanteenin enimmäiskoko (esim. 256 Mt) ja mikä on lähetettävän tiedoston enimmäiskoko.
- Virushälytykset. Tämän avulla voit määritellä sen, kertooko ohjelma muille käyttäjille, jos tietokoneelta löytyy virus.

- Poikkeukset. Voit antamalla tiedostopolun määritellä kohteet, joita ei tarkisteta. Antamasi poikkeukset vaikuttavat tosiaikaiseen ja ajastettuun tarkistukseen sekä myös itse käynnistettyyn tarkistukseen.
- Salasana. Tämän kautta voit antaa salasanan ja valita, mitkä ohjelman asetukset suojataan salasanalla. Valittavina suojatuiksi alueiksi ovat: Yleiset ohjelman asetukset, ohjelman asetukset, suojauksen hallinta, suojausasetukset, tarkistuksen hallinta, tarkistusasetukset, päivitysten hallinta sekä viruskaranteeni.
- Hiljainen/pelitila. Voit määritellä sen, miten usein ohjelma tulostaa näytölle viestejä toiminnastaan. Voit asettaa sen, näytetäänkö viestejä hiljaisessa/pelitilassa ja sen, näytetäänkö viestejä, jos jokin kokoruututilassa toimiva sovellus on käynnissä (kyseessä voi olla vaikka Power Point-esitys, peli tai elokuvan katselu).
- Tilarivi. Voit muuttaa asetuksissa olevien valintaruutujen avulla sitä, mitä ohjelman osia voidaan valvoa tilarivin avulla ja nämä ohjelman osat ovat: Tiedostojärjestelmäsuoja, sähköpostisuoja, selainsuoja, vertaisverkkosuoja, pikaviestinsuoja, verkkosuoja, käyttäytymissuoja, virustunnisteiden versio, ohjelmaversio, virustunnisteiden automaattiset päivitykset.
- Kieli. Voit valita, millä kielellä ohjelmaa käytetään. Valittavina on useita kieliä, myös suomi. Lisää kieliä saat asennettua ”asenna muita kieliä” –painikkeen kautta.
- Äänitehosteet. Voit muuttaa ohjelman käyttämiä äänitehosteita ja ensinnäkin sitä, että käytetäänkö lainkaan äänitehosteita.
- Ylläpito. Sivun kautta voit muuttaa sen, kuinka monta päivää väliaikaisia tarkistusraportteja säilytetään ennen poistamista.
- Yhteisö. Sivun kautta voit ilmoittautua ohjelman valmistajan verkkoyhteisön käyttäjäksi. Kun kuulut verkkoyhteisöön, annat ohjelmalle luvan lähettää tietoturvaan liittyviä tietoja ohjelman valmistajalle. Näistä tiedoista ei kuitenkaan voi tunnistaa tietojen lähettäjää.
- Vianhaku. Sivun kautta voi ratkoa erilaisia ongelmia. Voit mm. sallia rootkit-tiedostojen etsimisen käynnistyksen yhteydessä, sallia kiintolevyn suoraosoituksen käynnistyksen alussa tehtävän tarkistuksen aikana sekä ottaa käyttöön ohjelman itsepuolustusmoduulin.

5.2 F-Secure Client Security

F-Secure Client Securityn aloitusvalikko



Kuva 8. F-Securen aloitus-valikko

Tila-valikosta näkee millainen suojaus koneessa on tällä hetkellä.

Kuva 9. F-Secure-ohjelman tila-valikko

Tehtävät-valikossa on tehtävät, jotka auttavat yleisimpien ongelmien käsittelemisessä

Kuva 10. F-Securen tehtävät-valikko

Tilastot-valikon kautta voi tarkastella mitä tuote on tehnyt asennuksen jälkeen

Kuva 11. F-Securen tilastot-valikko

Tila-valikossa näet, että mitkä tarkistukset ovat käytössä ja mitkä ovat pois päältä tietokoneen, verkkoyhteyksien ja Internetin osalta.

Tehtävät-valikon sisältö:

- Tarkista, jonka avulla voit tarkastaa, että onko tietokoneella virus- tai vakoiluohjelmia. Voit myös tehdä täyden tietokoneen tarkistuksen, valita tietyt kohteet/kansiot, joita tarkastaa, voit myös muuttaa tarkistusasetuksia.
- Tarkista päivitykset, jonka avulla varmistat, että käytössä on uusimmat virustietokannat sekä ohjelmistopäivitykset.
- Avaa palomuurin portti. Tämän avulla voit avata portin palomuurin läpi kirjoittamalla palomuurisäännön nimen sekä portin numeron.

- Keskitetty hallinta. Tämän avulla voit tarkastella käytäntöä koskevia tietoja. Keskitetyn hallinnan avulla näet tietokoneen tiedot (WINS-nimi, DNS-alue, IP-osoite, yksilöllinen tunnus).
- Palauta poistettu tiedosto/ohjelma. Tämän avulla voit poistaa mahdollisessa eristyksessä olevan tiedoston tai ohjelman.
- Asetukset. Tästä valikosta saa nimensä mukaisesti muokattua asetuksia. Tämän valikon avulla voit muuttaa tila-valikossa olevia suojausasetuksia ottamalla ominaisuuksia käyttöön tai ottamalla ne pois käytöstä.
- Salli ohjelman käynnistyä. Tämän avulla voit tarkastella ohjelmia, jotka DeepGuard on analysoinut ja sallinut tai estänyt niiden käytön. Painaessa ”salli ohjelman käynnistyä” aukeaa valikko, jossa lukee: Ohjelma, polku, lupa, lisätty ja tyyppi kohdat. ”lupa”-kohdasta voit muuttaa hiiren oikean puoleista näppäintä painamalla sen, että ohjelma sallittu vai estetty.

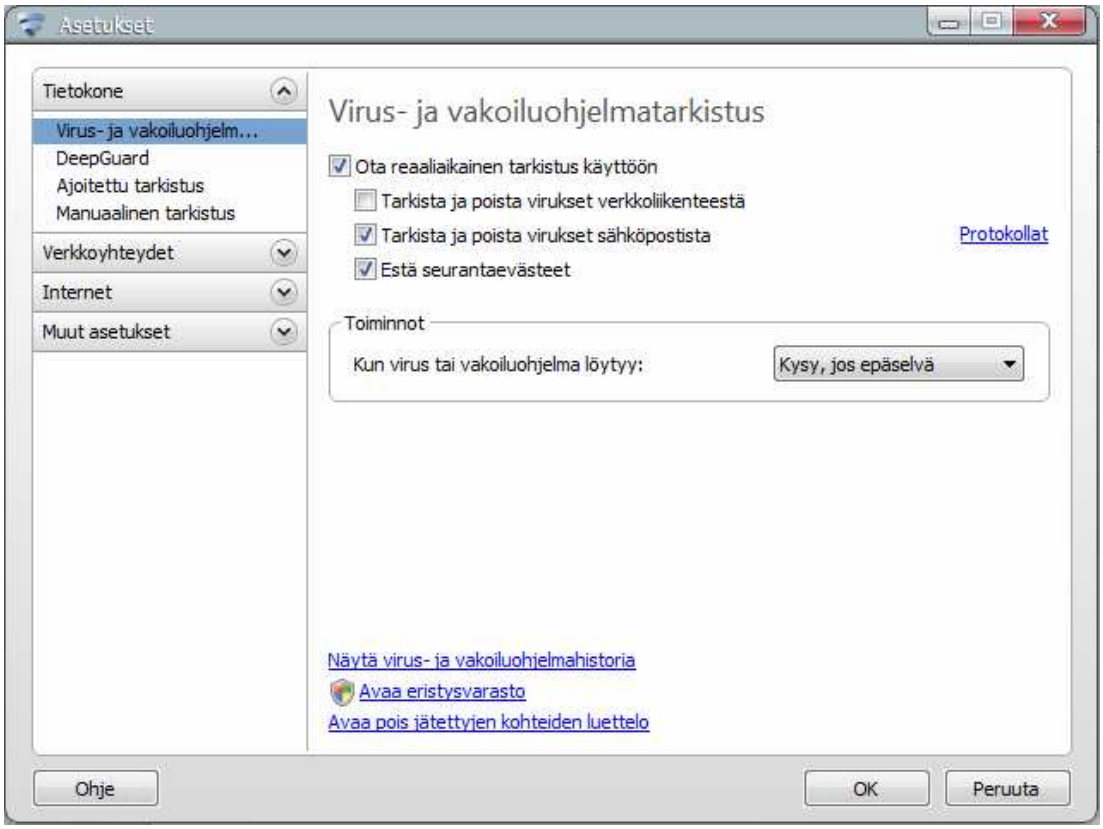
Tilastot-valikosta näet milloin viimeksi on tehty onnistunut päivitystarkastus ja sen, että onko tilaus voimassa. Näet myös, kuinka paljon virus- ja vakoiluohjelmia on tarkastettu ja puhdistettu, kuinka paljon ohjelmia on sallittu ja estetty käynnistymästä sekä sähköpostin tarkastuksen kelvolliset ja tyhjennetyt liitteet.

Tarkista-kohtaa painamalla voit valita, miten tietokoneen virus- ja vakoiluohjelmat tarkistetaan, tehdäänkö täydellinen tarkastus vai tarkistetaanko vain jokin tietty kohde. Valikon kautta voi myös muuttaa tarkistusasetuksia. Tämä tarkoittaa sitä, että voit valita tarkistetaanko vain tunnetut tiedostotyypit (nopea tapa tarkistaa), pakatut tiedostot ja käytetäänkö kehittynyttä heuristiikkaa (hidas tapa). Asetuksista voit myös muuttaa tapaa miten toimia, kun koneesta löytyy virus- tai vakoiluohjelma: Pyydetäänkö aina lupa, puhdistetaanko tiedostot, eristetäänkö tiedostot, poistetaanko tiedostot vai annetaanko vain raportti virus- ja vakoiluohjelmista.

Tarkista päivitykset –kohdasta voit tarkistaa, onko saatavilla uusia päivityksiä. Toisaalta tämän kautta on turha tarkastaa päivityksiä manuaalisesti, koska päivitykset etsitään monta kertaa päivässä automaattisesti.

Asetukset-valikko

Tässä kappaleessa on kerrottu vielä hieman tarkemmin ohjelman asetuksista.



Kuva 12. F-Securen asetukset-valikko

Tietokone-valikko

Asetuksien tietokone-kohdasta saat muutettua seuraavia asetuksia: Virus- ja vakoiluohjelmatarkistus, DeepGuard, ajoitettu tarkistus, manuaalinen tarkistus.

Virus- ja vakoiluohjelmatarkistuksesta saa muutettua sen, onko käytössä reaaliaikainen virus- ja vakoiluohjelmien tarkistus. Alasvetovalikosta saa valittua sen, mitä tehdään, kun tietokoneesta löytyy virus- tai vakoiluohjelma: Kysytäänkö, jos on epäselvää vai pyydetäänkö aina lupa.

DeepGuardista saat vaihdettua sen, onko DeepGuard päällä vai ei ja myös sen, käytetäänkö kehittynyttä prosessivalvontaa. DeepGuardin tarkoituksena on tunnistaa ja estää epäilyttävälle vaikuttava toiminta, joka voi vaarantaa tietokoneen. Kun haitallinen ohjelma löytyy, voidaan se käsitellä halutessa automaattisesti.

Ajoitetusta tarkistuksesta saa valittua sen, milloin tarkistus suoritetaan, valittavina on: päivittäin, viikoittain, kuukausittain ja minä viikonpäivänä se suoritetaan sekä myös sen, mihin aikaan. Ajoitettu tarkistus käyttää manuaalisen tarkistuksen asetuksia. Pakatut tiedostot tarkistetaan automaattisesti. Virukset, madot ja Troijan hevoset puhdistetaan automaattisesti.

Manuaalisen tarkistuksen kautta saa muutettua tarkistusasetuksia: Tarkistetaanko vain tunnetut tiedostotyypit, pakatut tiedostot (esim. zip) ja käytetäänkö kehittynyttä heuristiikkaa.

Verkkoyhteydet-valikko
Verkkoyhteydet-kohdasta saat muutettua seuraavia asetuksia: Palomuuri, sovellusten hallinta, tietomurtojen estäminen, puhelinverkkoyhteyden hallinta sekä kirjaus.

Palomuurista saa määriteltyä sen, onko palomuuri käytössä, minkä tasoinen on nykyinen palomuuriprofiili, onko se: Toimistotaso, langaton taso, kotikäyttötaso vai sallitaanko kaikki. Palomuuri-asetuksista voit muuttaa sen kuinka pienet IP-fragmentit estetään (käytössä on alle 128 tavua). Asetuksista voi valita myös IPv6-liikenteen suodatusasetukset ovatko ne estä vai normaali.

Sovellusten hallinnasta voi sallia tai estää ohjelmien Internet-yhteydet. Sovellusten hallinnan asetuksien yhteysyrityksiä-kohdasta voi valita sen, sallitaanko ja lisätäänkö ohjelma luetteloon ja valikosta saa myös määritettyä sen, kysytäänkö uusista sovelluksista.

Tietomurtojen estämisestä voi valita sen, otetaanko esto käyttöön. Valikosta vai valita myös sen, kun epäiltyjä tietomurtoja tulee, että estetäänkö ja kirjataanko yritys vai kirjataanko se ainoastaan. Voit myös laittaa ruksin kohtaan ”ilmoita epäillyistä tietomurtoyrityksistä”.

Puhelinverkkoyhteyksien hallinnasta määritellään se, otetaanko puhelinverkkoyhteyden hallinta käyttöön. Puhelinnumeroita voi lisätä numeroluettelo-välilehden numeroluetteloon, jos haluaa sallia tai estää puhelinverkkoyhteydet tiettyyn numeroon.

Kirjauksessa määritellään pakettien kirjausaika ja lokitiedoston enimmäiskoko. Kohdasta ”aloita kirjaus” voi aloittaa kirjauksen ja samasta kohdasta voi myös lopettaa sen. Kirjauksen-asetuksista voi myös määritellä hakemiston, johon kirjaus tallennetaan. Pakettien kirjauksen voi käynnistää, jos haluaa kerätä tietoja IP-verkkoliikenteestä.

Internet-valikko

Internet-valikon selauksen suojauksesta määritellään selauksen suojauksen ottaminen käyttöön. Kun selauksen suojaus on käytössä voidaan sen käyttö estää, kun Web-sivustossa on hyödyntämistä yrittävä toiminto sekä se, onko Web-sivusto luokiteltu haitalliseksi. Internet-asetuksista voi määritellä luotetut sivustot-kohdasta luotetut sivustot, eli luettelon haitallisista sivustoista, joiden esto on poistettu Internetiä selattaessa. Voit lisätä ja poistaa sivustot manuaalisesti. Selauksen suojaus on selaimen lisäosa, joka näyttää Web-sivustojen turvallisuusluokitukset hakuohjelman tulosluettelossa ja verkkosähköpostiviestien sisällössä. Selauksen suojauksen-valikosta voi määritellä, näytetäänkö luokitukset kohteelle: Hakukonetulokset (Google jne.) ja linkit Internet-postiin (Gmail, Hotmail jne.).

Muut asetukset-valikko

Valikosta voi määritellä seuraavien ominaisuuksien asetukset: Automaattiset päivitykset, Policy Manager –välityspalvelin, yhteys, lataukset, keskitetty hallinta, tietosuoja.

Automaattisista päivityksistä voi valita, otetaanko automaattiset päivitykset käyttöön, jolloin etsitään päivityksiä virustunnisteille, vakoiluohjelmatunnisteille sekä DeepGuardille. Automaattisista päivityksestä näkee, milloin viimeksi on päivitystarkastus tehty.

Policy Managerista saa lisättyä, poistettua ja muokattua uuden välityspalvelimen osoitteen. Osoitteen tulee olla muotoa http://proxy.example.com.

Yhteyksistä näkee verkon tilan, jossa lukee yhteys muodostettu. Yhteyksistä saa muutettua Internet-yhteyksien osalta sen, onko yhteys päällä jatkuvasti, kun havaitaan yhteys tai havaitaan tietoliikenne. Yhteydet-valikosta saa myös

määriteltyä HTTP-välityspalvelimen asetuksia: Onko HTTP-välityspalvelinta, määritelläänkö HTTP-välityspalvelin manuaalisesti vai käytetäänkö selaimen HTTP-välityspalvelinta.

Latauksista näkee, milloin erilaisia päivityksiä on asennettu. Tänään F-secureen on asennettu F-Secure Hydra Update, F-Secure Aquarius Update ja F-Secure DeepGuard Update.

Keskitetystä hallinnan kautta näkee tietokoneen tiedot: Wins-nimen, DNS-alueen, IP-osoitteen sekä yksilöllisen tunnuksen. Keskitetyssä hallinnassa tuoteasetukset ovat keskitetysti luotetun asiantuntijan etähallinnassa.

Tietosuojan kautta voi halutessaan osallistua ruudun ruksaamalla reaaliaikaisen suojauksen verkkoon lähettämällä nimettömänä tietoja palvelun parantamiseksi.

5.3 Tietoturvaohjelmien ominaisuuksien vertailu

Avast! on omasta mielestäni sekä luettujen tietojen perusteella luultavasti paras saatavilla oleva ilmainen virustorjuntaohjelma. Opinnäytetyössäni käytössäni oli Avast! 5 versio 5.0.667.

Yrityksille on saatavilla myös maksullinen versio Avast! Professional Edition. Opinnäytetyössäni käyttämä Avast! 5 on huomattavasti helppokäyttöisempi kuin Avast! 4. Jos käytössäsi on vielä Avast! 4, saat helposti asennettua uuden version, vanhaa versiota ei tarvitse poistaa vaan se asentuu helposti uuden päälle.

Avast! on kehitetty Windows- ja Linux-käyttöjärjestelmille. Virustorjuntaohjelma on suunniteltu erityisesti koti- ja ei-kaupalliseen käyttöön. Avast!-ohjelma on saatavilla monilla eri kielelle, myös suomeksi. Myös F-Secure Client Security on saatavilla suomen kielellä. Avast! nimi tulee ”anti-virus advanced set” sanoista.

Avast! Sisältää mm. tehokkaan taustasuojauksen, P2P ja IM (MSN jne.) –suojan, verkkosuojauksen (matoja jne. vastaan), web-suojauksen, automaattiset päivitykset sekä virusten puhdistustyökalun.

Avast! Home Editionin lisenssi on voimassa aina vuoden. Tämän jälkeen uuden lisenssin pyytäminen tarvitsee tehdä Avastin rekisteröintisivulta, jolloin lisenssiavain lähetetään sähköpostiin. Uusi lisenssiavain tulee sähköpostiin 24 tunnin kuluessa.

Avastin asetukset-valikko on ulkonäöltään ja asetusten muuttamisen kannalta helppokäyttöisempi vähemmän asioita tuntevalle henkilölle kuin F-Secure Client Security. Eri asetuksia muuttaessa on aina muutaman rivin selitys siitä, mitä asetuksia tietyn sivun kautta voi muuttaa, tällöin tiedät helpommin, mitä asetuksia olet muuttamassa. Tällaista mahdollisuutta ei F-Secure Client Securityssä ole saatavilla.

F-Secure Client Security -ohjelma on helppokäyttöinen ja kaikki tarvittavat toiminnot löytyvät helposti. Opinnäytetyössäni käytin F-Secure Client Securityn versiota 9.01. Olen huomannut F-Securen Client Securityn käytön aloittamisen jälkeen, että koneeni suorituskyky on toisinaan hieman hidastunut ja ainakin Internet-selaimen avaus kestää kauemmin, tätä en aiemmin ollut huomannut, kun käytettävissäni oli Avast! Antivirus. En sitten tiedä varmuudella, onko tämä F-Securesta johtuvaa. F-Secure Client Security kyllä on tiedostokooltaan isompi ohjelma kuin Avast. Jos tietokoneessa on aikaisemmin ollut jokin toinen tietoturvaohjelma, pitää tämä poistaa ennen F-Secure Client Securityn asentamista.

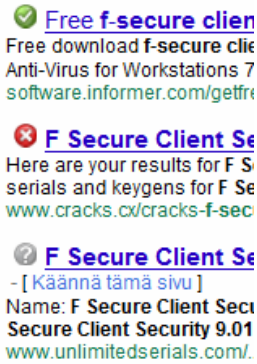
Ohjelma sisältää virusten- ja vakoiluohjelmien torjunnan, palomuuri- ja hyökkäyksenestotoiminnon sekä keskitetyn hallintajärjestelmän työasemille ja kannettaville tietokoneille.

- Palomuuri, jossa tietomurtojen esto
- Suojaus vakoiluohjelmilta
- Automaattiset tietoturvatasot

F-Securen uusimmat virustorjuntaohjelmistot ovat F-Secure Internet Security 2011 ja F-Secure Client Security 9.

F-Securen kotisivuilta löytyy Online Virus Scanner (http://www.f-secure.com/fi_FI/security/security-lab/tools-and-services/online-scanner/). Online Scannerin avulla voi tarkastaa, onko tietokone haittaohjelmien saastuttama. Ennen kuin voit aloittaa Online Scannerin käytön, pitää asentaa lisäosa selaimeen.

F-Securen tietoturvaohjelmaa käyttäessä ja Googlen haulla tietoa etsiessä näyttää haku, mitkä sivustot ovat turvallisia: ”sivusto on turvallinen”, ”sivusto on haitallinen”, ”sivustoa ei ole analysoitu vielä”.



Kuva 13. Googlen hakutulokset F-Secure ohjelmaa käyttäessä

F-Securen tehtävä-valikossa on laajemmin erilaisia vaihtoehtoja valittavissa, mitä haluaa tehdä, kuin Avastin vastaavanlaisia asetuksia käsittävässä tietokoneen tarkistus-kohdassa.

F-Securen tilastot-valikko on selkeämpi kuin Avastin vastaava valikko. F-Securen tilastot (tarkistetut, puhdistetut tiedostot, sähköpostin tarkistuksen kelvolliset ja tyhjennetyt liitteet sekä sallitut ja käynnistymästä estetyt ohjelmat) näkee pelkästään yhdellä klikkauksella. Avastissa saman asian tekeminen tehdään alasvetovalikosta valitsemalla esim. sähköpostisuojan, josta näkee kuinka paljon sähköpostiviestejä on tarkistettu ja tyhjennetty. Avast on hieman monimutkaisempi käyttää, mutta tarkistusajankohdat näkee tarkemmin eli nähtävissä on kuinka paljon, minä päivänä sekä mihin aikaan sähköpostiviestejä on tarkistettu.

Tietoturvaohjelmien tarkistusraportteja tutkiessa huomasin, että Avast avaa tarkistusraportin itse ohjelmassa, kun taas F-Secure avaa sen Internet-selaimeen, tämän avaaminen kestää hetken kauemmin, kuin Avastissa raportin avaaminen. Se hyvä puoli Internet-selaimeen avaavassa ohjelmassa on, että tilastot tulevat tarkasti esille eli näet kaikki tarkistetut, tarkistamattomat tiedostot, tulokset, toiminnot (mm.

puhdistukset, poistetut ja eristetyt) sekä käynnistyssektorit. Avast ei ilmoita näin tarkasti tilastoja. Toisaalta, jos ei kaipaa niin tarkkoja tilastotietoja tarkistuksesta, niin on Avast silloin parempi, kun tarkistusraportin näkee siis heti ohjelmaan avautuvalla sivulla ja siitä näkee myös pääasiassa tärkeimmät ja tarpeellisimmat tiedot.

Ohjelmiin tutustumisen ja niiden tutkimisen jälkeen suosittelisin ennemmin Avastia peruskäyttäjän tietokoneeseen sen helppokäyttöisyyden ja pienemmän kuormittavuuden vuoksi. F-Secure Client Security sopii paremmin ammattilaisen ja tietoturva-asioista enemmän tietävän ja ammattilaisen käytettäväksi eli ainakin yritysten käyttöön. F-Secure Client Security kuormittaa siis tietokonetta enemmän kuin Avastin tietoturvaohjelma. Joten vanhemmille koneille suosittelen Avastin käyttöä, uudemmalla tietokoneella F-Securen ohjelmankin pitäisi toimia moitteettomasti.

6 YHTEENVETO JA JOHTOPÄÄTÖKSET

Opinnäytetyöni tarkoituksena on kertoa tärkeimpiä asioita tietoturvasta, virus- ja haittaohjelmilta suojautumisesta sekä erilaisista tietoturvaohjelmista. Opinnäytetyössäni keskityin tietoturvan ja tietoturvaohjelmien perusteiden kertomiseen. Opinnäytetyöni pitää sisällään tietoturvan ja tietoturvaohjelmien perusteita sekä tietoturvaohjelmien vertailua. Tietoturvaohjelmien vertailussa keskityin kahteen parhaimpaan saatavalla olevaan ohjelmaan. Opinnäytetyöni tarkoituksena on tutustuttaa lukija tietoturvan perusasioihin.

Opinnäytetyötä aloittaessa tutustuin erilaisiin tietoturvaohjelmiin, joista sitten päädyin valitsemaan mielestäni kaksi parasta saatavilla olevaa tietoturvaohjelmaa, tarkoituksena oli valita ohjelmat niin, että toinen näistä olisi kaupallinen ja toinen ei-kaupallinen. Tässä vaiheessa hain tietoa myös tietoturvan perusteista ja tietoa etsin suurimmaksi osaksi Internetistä, mutta tutustuin myös tietoturvaa käsittelevään kirjaan.

Seuraavassa vaiheessa aloitin tutustumaan syvemmin tietoturvaohjelmiin ja kasaamaan tietoa Internetistä. Materiaalin etsiminen sujuikin melko helposti. Varmaan vaikeinta opinnäytetyössäni oli miettiä, missä järjestyksessä asioita halusin kertoa ja minkä asioiden kertomiseen rajaisin opinnäytetyöni.

Opinnäytetyöni lopputuloksena voidaan todeta, että tietoturvan päivittäminen, siitä huolta pitäminen ja tieturvaohjelman asentaminen omalle koneelle on suositeltavaa. Ei pidä sokeasti luottaa omaan tietoturvaohjelmaan. Vaikkakin tietoturvaohjelman viruspäivityksien pitäisi aina olla ajan tasalla, voi yhtäkkiä tullakin jokin uusi virus tai haittaohjelma, jota ei ole vielä tunnistettu ja tällöin viruspäivityksetkään eivät asennu automaattisesti. Suosittelisin Avastin asentamista peruskäyttäjän tietokoneelle sen helppokäyttöisyyden takia, F-Securen ohjelma sopii paremmin ammattilaisen käyttöön.

LÄHTEET

/1/ Suomen Internetopas - Tietoturva. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.internetopas.com/yleistietoa/tietoturva/

/2/ Kansalaisen mikrotuki. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.kansalaisenmikrotuki.fi/?tietoturva/virukset

/3/ Suomen Internetopas – Viruksilta suojautuminen. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.internetopas.com/yleistietoa/virukset/suojautuminen/

/4/ CERT-FI – Suojautuminen phishing-hyökkäykseltä. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.cert.fi/ohjeet/2005/ohje-2005-01.html

/5/ Viestintävirasto – Suojautuminen haittaohjelmilta. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/haittaohjelmat/suojautuminenhaittaohjelmilta.html

/6/ Viestintävirasto – Virustorjunta. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/virustorjunta.html

/7/ Wikipedia – Avast. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://fi.wikipedia.org/wiki/Avast!

/8/ Wikipedia - Avira AntiVir. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://fi.wikipedia.org/wiki/Avira_AntiVir

/9/ Wikipedia – AVG Anti-Virus. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://fi.wikipedia.org/wiki/AVG_Anti-Virus

/10/ Wikipedia – F-Secure. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://fi.wikipedia.org/wiki/F-Secure

/11/ Wikipedia – Norton AntiVirus. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://fi.wikipedia.org/wiki/Norton_AntiVirus

/12/ Wikipedia – McAfee. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://fi.wikipedia.org/wiki/McAfee

/13/Panda Internet Security. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.pandasecurity.com/finland/homeusers/solutions/internet-security/

/14/ Tietoturvaa ilmaiseksi – Mitä on tietoturva. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.lindstorm.org/tietoturva/tietoturva.html

/15/ Laaksonen M., Nevasalo T. & Tomula K. Yrityksen tietoturvakäsikirja Ohjeistus, toteutus ja lainsäädäntö. Edita Publishing Oy, 2006. s 17-18. [Viitattu 2.5.2011].

/16/ Viestintävirasto – Sähköisen viestinnän tietoturva ja –suoja. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.ficora.fi/index/saadokset/lait/svt.html

/17/ Viestintävirasto – Velvollisuudet ja oikeudet. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/svt/teleyritys/velvollisuudetjaoikeudet.html

/18/ Henkilörekisteri. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.cs.tut.fi/~jkorpela/hlorek.html#rekisteri

/19/ Tietosuojavaltuutetun toimisto – sanastoa. [Viitattu 2.5.2011]. Saatavissa: http://www.tietosuoja.fi/27247.htm

/20/ Viestintävirasto – Tietoa yhteisötilaajille. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/svt/yhteisotilaaja.html

/21/ Viestintävirasto – Tietoturvallisuuteen liittyvät velvollisuudet ja oikeudet. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/svt/yhteisotilaaja/velvollisuudetjaoikeudet.html

/22/ CERT-FI – Langattomien lähiverkkojen turvallisuus. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://www.cert.fi/ohjeet/2002/P_6.html

/23/ Wikipedia – Langattoman lähiverkon tietoturva. [Verkkodokumentti]. [Viitattu 2.5.2011]. Saatavissa: http://fi.wikipedia.org/wiki/Langattoman_lähiverkon_tietoturva