Opinnäytetyö (AMK)

Tietojenkäsittely

Sähköisen liiketoiminnan järjestelmät

2013

Siina Mohammad

TIETOTURVALLINEN TYÖASEMAKOKOONPANO. CASE: AGENTEQ SOLUTIONS OY JA SUOMEN TALOKESKUS KONSERNI

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Sähköisen liiketoiminnan järjestelmät

Marraskuu 2013 | 27

Ohjaaja Minna Paakki

Siina Mohammad

TIETOTURVALLINEN TYÖASEMAKOKOONPANO. CASE: AGENTEQ SOLUTIONS OY JA SUOMEN TALOKESKUS KONSERNI

Tämän opinnäytetyön tavoitteena on luoda menetelmä, jonka avulla Agenteqin ja Suomen Talokeskus-konsernin työasemat jatkossa turvataan. Tarve projektille ilmaantui kun koko konsernin työasemien tietoturva haluttiin yhtenäistää. Tarkoituksena on parantaa molempien yritysten tietoturvaa ja suojata työntekijöiden sekä asiakkaiden tietoa. Aluksi tämän projektin tulokset tullaan ottamaan käyttöön Agenteqissa, jossa testataan toimivuus ja vasta tämän jälkeen laajennetaan koko konsernille.

Tutkimus tehtiin toimeksiantona Agenteq Solutionsille joka on ohjelmistoyritys. Tehtävänä oli luoda dokumentaatiota jota jatkossa käytetään koko konsernissa ja jota on helppo kehittää eteenpäin. Dokumentaatiolla myös muutkin pk-yritykset voivat kehittää tietoturvakäytäntöjään.

Työn teoriaosuudessa esitellään peruskäsitteitä ja määritellään aiheeseen liittyviin termit. Lisäksi käsitellään tutkimushetkellä oleva tilanne konsernissa ja selvitetään millaisia tietoturvauhkia yritykseen voi kohdistua. Eri ohjelmistoja vertaillaan ja niistä tehdään kartoitus mikä niistä otetaan käyttöön yrityksessä. Empiirisessä osuudessa otetaan käyttöön konsernille sopivat ohjelmistot ja työkalut.

Opinnäytetyön ansiosta Agenteq Solutionsin työasemien tietoturva ja niihin liittyvät dokumentaatiot selkenivät. Prosessin aikana selvisi myös, että yrityksen tietoturvassa on vielä paljon parannettavaa ja muita osa-alueitakin mitä voisi tutkia ja kehittää paremmaksi.

ASIASANAT:

Suomen Talokeskus, Agenteq Solutions, työasema, tietoturva

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme in Information Technology | e-Business Systems

November 2013 | 27 pages

Instructor Minna Paakki

Siina Mohammad

CONFIGURATING SECURE WORKSTATIONS. CASE: AGENTEQ SOLUTIONS AND SUOMEN TALOKESKUS GROUP

The main goal of this thesis is to create a method how to secure Agenteq and Suomen Talokeskus groups' workstations in the future. The need for this project occurred when the named companies wanted to unify their workstation security policies. The purpose of this was to improve both companies' security and protect employees' as well as customers' sensitive data.

The study was done for a software company and the main task was to create documentation which the company can use in the entire corporation and which can be easily developed further. Other small and medium size companies can also use this document for their own purpose.

The theory presents the main concepts in thesis and defines the general topics and concepts. After that, the situation at the time of research is explained and the potential security threats for corporation are analyzed closer. The empirical part was conducted to Agenteq Solutions and it included software initialization.

After thesis company identified what problems and security risks they have. During the process it became clear what parts need improvements.

KEYWORDS:

Suomen Talokeskus, Agenteq Solutions, workstation, computer security

SISÄLTÖ

KUVAT

1 JOHDANTO

Opinnäytetyön tavoitteena on perehtyä mahdollisiin työasemien tietoturvauhkiin joita yritykselle voisi kohdistua ja toteuttaa suunnitelma, jolla torjutaan uhat. Tutkimuksessa tullaan tutustumaan levyjen salauksiin, yrityksille tarjottaviin virustorjuntaohjelmistoihin ja kolmannen osapuolen ohjelmistojen automaattisiin päivitysohjelmiin. Työssä selvitetään mikä näiden kolmen yhdistelmä olisi hyödyllisin yritykselle.

Toimeksiantaja on Agenteq Solutions. Yritys halusi tämän työn tehdyksi, jotta koko konsernilla olisi dokumentaatio, miten työasemien tietoturva on toteutettu. Samaa dokumentaatiota tullaan käyttämään sekä Agenteq Solutionsissa että Suomen Talokeskuksessa, joka on Agenteq Solutionsin pääomistaja.

Työn alussa esitellään keskeiset käsitteet työasemien tietoturvallisuudesta. Keskivaiheessa tuodaan esille työasemien tietoturvallisuusuhkia ja suojausmenettelyitä. Opinnäytetyöhön valitaan eri ohjelmistoja joita vertaillaan keskenään ja lopuksi valitaan sopivin ohjelmisto. Loppuvaiheessa esitetään konsernille toteutettu suunnitelma ja tarkastellaan miten toteutus onnistui.

Saatuani toimeksiannon asetin itselleni tavoitteita. Ensisijaisesti pyrin parantamaan toimeksiantajan järjestelmien tietoturvallisuutta ja samalla kirjoittamaan dokumentaation, joka hyödyttäisi toimeksiantajaa ja mahdollisesti muitakin pk-yrityksiä. Muina tavoitteina pidin henkilökohtaisen tietoturvaosaamisen kehittymistä.

2 TUTKIMUKSEN TAUSTA

2.1 Toimeksiantaja

Agenteq Solutions Oy on perustettu vuonna 1999 kahden miehen toimesta. Toiminta alkoi erilaisten asiantuntijatehtävien ja tuotantoprojektien kautta joita tehtiin Suomen Talokeskukselle sekä Nokialle. Tärkein palvelu mitä yritys tarjoaa, on Tampuuri-ohjelmisto joka on tarkoitettu kiinteistöalan yrityksille. Nykyään yritys kehittää ja ylläpitää asiakkaillensa laajoja ja liiketoiminnallisesti tärkeitä järjestelmiä. (Agenteq 2013) Yrityksen liikevaihto oli vuonna 2011/12 n. 6,4 milj. euroa. (Finder, 2013)

Vuonna 2010 Suomen Talokeskus Oy osti koko Agenteq Solutions Oy:n osakekannan ja näin Agenteqista tuli Suomen Talokeskus Oy:n tytäryhtiö. Yritysten liiketoiminta on itsenäistä, mutta joitakin toimintoja yritetään yhdistää konsernissa. Yksi näistä on juuri tietojärjestelmät ja työasemien tietoturvallisuus jota tutkitaan tässä opinnäytetyössä. (Agenteq 2013)

2.2 Työn tavoite

Lähtiessäni opintonäytettä tekemään kävimme keskustelua it-päällikön kanssa työn tavoitteista. Ensimmäinen tavoite oli yhtenäistää konsernin turvallisuusohjelmistot ja niiden hallinta. Näin saamme helpotettua ja automatisoitua tiettyjä toimintoja jolloin it-tiimikin pystyy keskittymään tärkeämpiin tehtäviin. Huomioon otetaan myös tulevaisuuden näkymät, koska yrityksen liiketoiminta kasvaa ja sinne rekrytoidaan yhä enemmän uusia työntekijöitä. Toinen tavoite oli henkilökohtainen. Työn kirjoittaja on aina ollut kiinnostunut tietoturvallisuudesta, joten työ tulee olemaan mielenkiintoinen ja opettavainen. Järjestelmänasiantuntijana usein päädytään kuitenkin sellaisiin tehtäviin joissa tietoturvaosaaminen on tärkeää. Nyky-yhteiskunnassa tietoturvan painoarvo on kasvanut, joten sen osaaminen nostaa työntekijän markkina-arvoa ja lisää yrityksen luotettavuutta asiakkaiden silmissä.

2.3 Työn valmistelu

Työtä alettiin valmistelemaan niin, että it-päällikön kanssa käytiin palavereja miten voitaisiin lähteä rakentamaan turvallista työasemakokoonpanoa, jonka tietoturvallinen taso olisi korkea mutta ei kuitenkaan haittaisi käyttäjän jokapäiväistä työtä. Päästiin tulokseen että kaiken pitäisi toimia automaattisesti, joka helpottaisi it-tiimin työtä ja samalla antaisi riittävän suojan uhilta.

Minulla ja it-päälliköllä oli jo ajatuksena mitä ohjelmistoja tulemme käyttämään ja mahdollisesti vertailemaan keskenään, jotta teemme viimeisen päätöksen. Halusimme pitää vertailulistan sopivan pienenä ja ottaa siinä huomioon ohjelmistot jotka olivat jo ennestään tuttuja it-tiimille jolloin niiden käyttö oli nopeampaa ja helpompaa.

3 KESKEISET KÄSITTEET

3.1 Tietoturva

Tietoturvallisuudella tarkoitetaan yrityksen tietojen, järjestelmien, palveluiden ja tietoliikenteen suojaamista tietoturvauhilta. Tietoturvan tavoitteena on turvata yrityksen data, pitää se luotettavana ja ainoastaan tietoon oikeutettujen henkilöiden saatavissa. (Suomen internetopas, 2013) Tietoturvallisuuden uhkia on nykyään paljon. Niitä on esimerkiksi henkilökohtaisen yksityisyyden loukkaukset, roskapostit joita lähetetään sähköpostitse, teollisuusvakoilu, piratismi, tietokonevirukset, verkkoterrorismi ja maiden välinen elektroninen sodankäynti. (Wikipedia, 2013)

IT-päällikön kanssa käydyissä keskusteluissa tultiin siihen tulokseen että suurimmat riskit jotka voivat kohdistua Agenteq Solutionsille ja Suomen Talokeskukselle ovat haittaohjelmat joilla päästään käsiksi yrityksen tai asiakkaan omistamaan tietoon, palvelinestohyökkäykset joilla pyritään häiritsemään yrityksen liiketoimintaa tai fyysisen laitteen, kuten kannettavan katoaminen tai varastaminen.

3.2 Työasema

Terminä työasema yrityksessä tarkoittaa päätelaitetta, jonka tarkoituksena on tarjota käyttäjälle rajapinta palveluihin ja ohjelmistoihin joita työtehtävässä tarvitaan. Useimmiten nämä päätelaitteet ovat joko pöytäkoneita tai sitten kannettavia. Nykyään myös tablettien käyttö työvälineenä on lisääntymässä. (Vahti, 2010)

Työasemat ovat suurimpia uhkia yrityksen verkossa, koska käyttäjät voivat tahattomasti tai tahallisesti aiheuttaa ongelmatilanteita. Työasemien tietoturvaa pystyy parantamaan opastamalla käyttäjiä ja päivittämällä niissä käytettyjä ohjelmistoja. Tähän asti yrityksessämme käyttäjät ovat olleet itse vastuussa oh-

jelmistojen päivittämisestä, mutta juuri tähän haetaan ratkaisua tämän opinnäytetyön avulla.

3.3 Työasemaan kohdistuvat uhat

Työasemaan voi kohdistua monenlaisia uhkia, kun sitä käytetään sekä työskentelyyn että henkilökohtaiseen käyttöön. Tässä pääluvussa tullaan käymään läpi tietoturvauhkia jotka voivat kohdistua yrityksen työasemiin.

Tietoturvan tärkeyttä ei voi yrityksissä nykyään painottaa riittävästi, koska niihin kohdistuu usein paljon hyökkäyksiä jotka voivat vahingoittaa liiketoimintaa. Yleensä hakkerit hyökkäävät tunnettujen yritysten järjestelmiin mutta tämä ei tarkoita sitä että pienen yrityksen ei kannata suojata järjestelmiään.

Haittaohjelmat alaluvussa käydään läpi yleisimmät haittaohjelmat ja se miten ne voivat tarttua työasemaan. Haittaohjelmatyypeistä käydään läpi virukset, madot, troijalaiset, vakoiluohjelmat, rootkitit ja botit. Haittaohjelmatyypeistä mikä vain voi saada aikaan tuotannon pysähtymisen ja siksi työasemien käyttäjien tulisi asennoitua tietoturvaan vakavasti. Kuvassa 1 on nähtävillä haittaohjelmat vuodelta 2013 jonka on teettänyt Panda Security-tietoturvayritys. Yritys on 3 kuukauden ajalta kerännyt yli 6,5 miljoonaa haittaohjelmanäytettä.

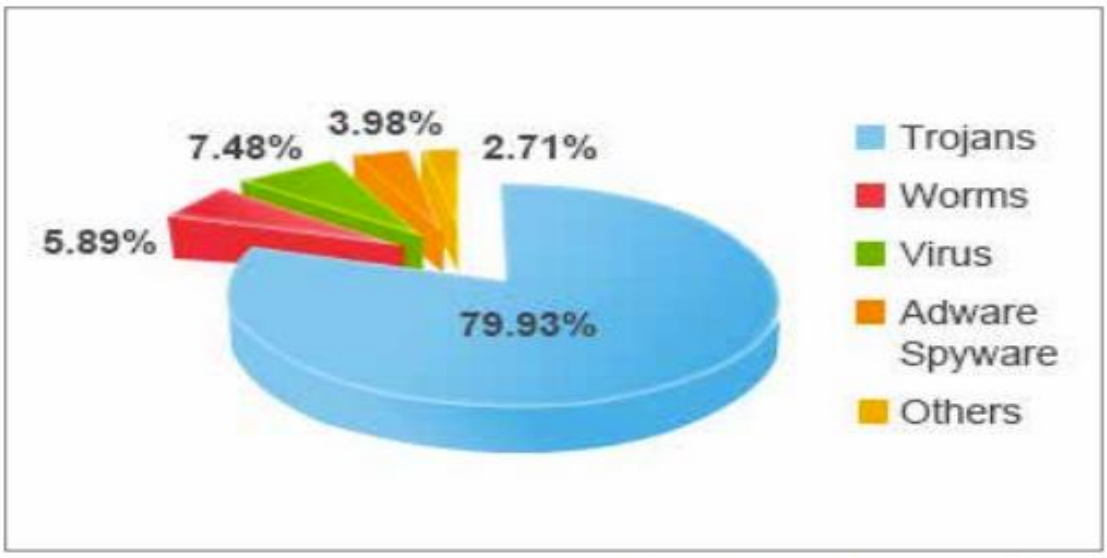


FIG.5. *MALWARE INFECTIONS BY TYPE IN Q1 2013.*

Kuva 1. Panda Securityn raportti vuodelta 2013.

Varkaus- ja katoamis-luvussa käydään läpi mitä riskejä yritykseen kohdistuu kun kannettava joko varastetaan tai kadotetaan. Yleensä työasemissa sijaitsee yrityksille tärkeitä ja salaisia dokumentaatioita jotka voivat paljastaa mm. yritysten tietojärjestelmien tietoja tai talouslukuja. Nämä paljastumiset voivat aiheuttaa sitten sen, että yritys menettää asiakkaidensa luottamuksen joka voi johtaa konkurssiin.

Osiossa datan menetys käsitellään mitä vaikutuksia on jos yrityksen dataa häviää tai korruptoituu. Tämän jälkeen tarkastellaan sitä miten siihen voi valmistua jotta pystytään tietojärjestelmät palauttamaan toimintakuntoon nopeasti ilman suuria käyttökatkoksia.

3.3.1 Haittaohjelmat

Haittaohjelma on ohjelma, jonka tarkoituksena on tahallisesti aiheuttaa vahinkoa käyttäjälle. Haittaohjelmia voi jaotella eri kategorioihin sen mukaan miten ne leviävät, suoritetaan tai mitä ne tekevät, kun ne pääsevät dataan käsiksi. (Wikipedia, 2013)

Tietokonevirukset ovat haittaohjelmistoista vaarallisimpia, koska ne voivat aiheuttaa kaikista eniten vahinkoa. Tietotekniikan alussa nämä haittaohjelmat tarttuivat käyttäjien työasemissa sijaitseviin ohjelmistojen kansioihin tai jopa käyttöjärjestelmän käynnistysohjelmiin. Myöhemmin ne alkoivat levitä Microsoftin Excelin ja sähköpostin välityksellä. Yleensä virus on ohjelmoitu tuhoamaan työaseman tärkeitä tiedostoja ja häiritsemään käyttäjän työskentelyä työasemalla. (Vahti 3/2004)

Madot pystyvät leviämään ilman muiden ohjelmien apua yleensä jonkin tietoturva-aukon välityksellä jonka hakkeri on löytynyt järjestelmästä tai sitten se huijaa käyttäjää suorittamaan sen. Yleensä ne leviävät sähköpostin liitteenä jonka käyttäjä avaa, jolloin ohjelma suoriutuu ja kerää tietokoneesta tietoja jotka se lähettää eteenpäin. (Vahti 3/2004)

Troijalainen on tietokoneohjelma, jonka tehtävänä on avata takaportti järjestelmään, jotta hyökkääjä pääsee murtautumaan koneelle. Murtautumisen jälkeen hyökkääjällä on yhteys aina avoinna kohdekoneeseen ja voi käyttää sitä muihin hyökkäyksiin toisiin järjestelmiin. Troijalaiset voivat myös kerätä tietoja kuten salasanoja, sähköposteja ja lähettää ne eteenpäin. Haittaohjelma voi olla osana toista ohjelmaa jolloin sen havaitseminen on vaikeaa. Jotkut troijalaisista levittävät myös muita haittaohjelmia kuten mainosohjelmia ja viruksia. [Vahti 3/2004]

Vakoiluohjelma eli (engl. spyware) on haittaohjelma, joka kerää tietoja tietokoneesta ja käyttäjästä välittää ne verkon kautta ohjelman kehittäneelle taholle. Tiedot jotka hakkeria kiinnostaa voivat olla esimerkiksi käyttäjän selaamat internet-osoitteet, tunnukset, sähköpostiosoitteet, salasanat tai luottokorttitiedot. Yleisin tapa miten vakoiluohjelma asentuu on toisen ohjelman ohessa ilman käyttäjän lupaa tai tietämystä. (Vahti 3/2004)

Rootkit on ohjelmisto, joka asentuu tietokoneelle hyökkääjän saatua sen hallintaansa. Rootkit-ohjelmistoa käytetään yleensä muiden haittaohjelmien piilottamiseen käyttäjiltä ja viruksentorjuntaohjelmistoilta. Rootkitit pyrkivät piilottamaan itsensä käyttöjärjestelmään jonkin siinä olevan tietoturva-aukon avulla ja tämän jälkeen ne piilottavat tietokoneella olevat haitalliset prosessit tai ohjelmat. Rootkit voi myös asentua käynnistyssektorille jolloin sen poisto vaikeutuu. (Wikipedia, 2013)

3.3.2 Varkaus tai katoaminen

Kun kyseessä on kannettava työasema niin riski sen kadottamiseen tai varastamiseen on suuri. Usein yritysten työntekijät matkustelevat paljon jolloin kannettava voi unohtua julkiseen paikkaan. Pöytäkoneita harvoin varastetaan tai kadotetaan, koska ne sijaitsevat toimitiloissa joihin harvoin luvattomilla on pääsyä.

Katoamiseen tai varkauteen ei voi muulla tavalla varautua kuin suojaamalla käyttöjärjestelmään kirjautumisen salasanalla. Tähän toimenpiteeseen voi joko

käyttää Windowsin omaa kirjautumisjärjestelmää tai sitten kolmannen osapuolen ohjelmistoja jotka suojaavat jopa käynnistyssektorin ja BIOSin jolloin varas ei pääse käynnistämään konetta ulkoiselta levyltä tai CD:ltä. Levyn kryptaus myös ajaa samaa asiaa, koska silloin varas ei pysty näkemään tiedostojen sisällön selväkielisenä jos hän pääsee käyttöjärjestelmään käsiksi. Levyn kryptauksessa on myös omat vaaransa. Jos käyttäjä hävittää palautusavaimen tai salauksen salasanan niin levyn toimintakuntoon laittaminen on lähes mahdotonta, koska salausta ei pystytä purkamaan jolloin kaikki data levyllä tai levyosiolla häviää. (Hakala 2006, 137)

3.3.3 Datan menettäminen

Datan menettämisellä voi olla suuria negatiivisia vaikutuksia yrityksen liiketoimintaan. Datan menetyksellä tarkoitetaan tiedoston tuhoutumista tai hävittämistä joka yleensä johtuu monesti käyttäjän omasta virheestä tai huolimattomuudesta. Myös datan korruptoituminen voi aiheuttaa ongelmia yritykselle. Datan menetykseen pystytään suojautumaan riittävän useasti otetuilla varmuuskopioilla. (Ruohonen, 2002)

Agenteqin palvelimilla sijaitsee paljon asiakkaiden omistamaa dataa jonka menettäminen tarkoittaisi asiakassuhteen päätöstä ja maineen menetystä. Myös omien työntekijöiden järjestelmien ja työasemien varmistuksen pitäisi olla kunnossa, koska nekin sisältävät tärkeää dataa kuten esimerkiksi lähdekoodeja ja dokumentaatioita. Näiden menetys tarkoittaisi usean työtunnin menetyksen, joka näkyisi negatiivisena liikevaihdossa.

Agenteqissa työasemat varmuuskopioidaan viikossa kerran ulkoiselle kiintolevylle ja lisäksi käyttäjiä on ohjeistettu kopioimaan omalta koneelta tärkeät tiedostot verkkolevylle päivittäin. Jos työtekijältä katoaa tietty tiedosto, niin se palautetaan joko työaseman imagesta tai sitten sen voi palauttaa verkkolevyltä johon sen on manuaalisesti varmuuskopioinut.

4 VIRUSTORJUNTAOHJELMISTOJEN VALINTA

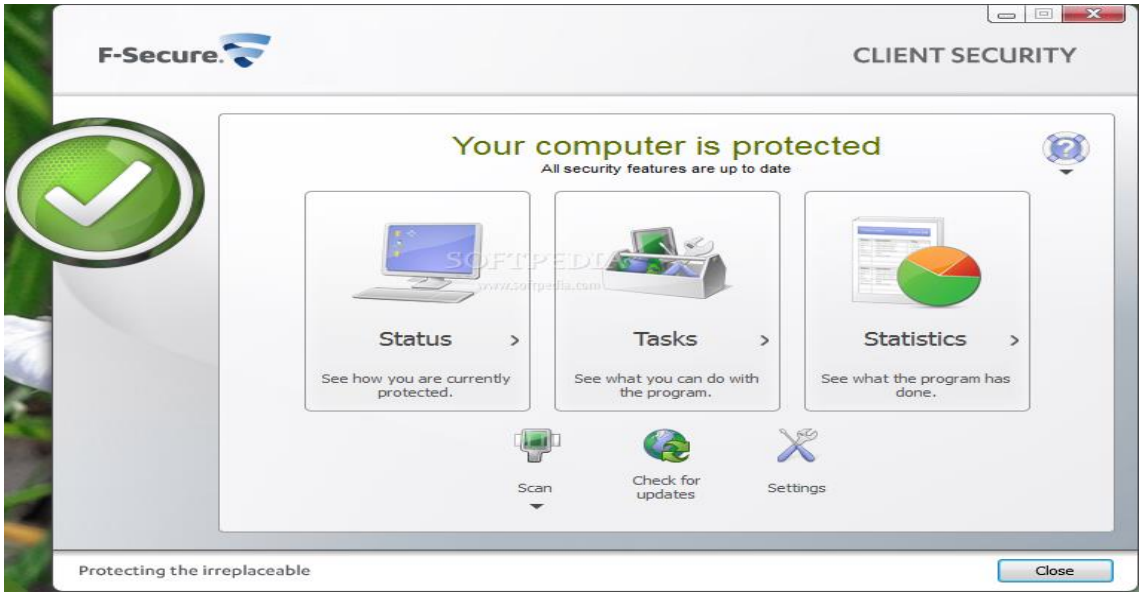
Nykyään yrityksillä ja yksityishenkilöillä on varaa valita useasta eri tietoturvaohjelmistosta. Kotikoneille tarkoitetut virustorjunnat käyvät myös yritysten työasemiin, mutta useasti yritysten työasemat vaativat toimintoja joita ei kotikoneille tarkoitetuista ohjelmistoista löydy kuten työasemien keskitetty hallinta.

Tietoturvaohjelmaa valitessamme IT-päällikön kanssa päädyimme siihen, että 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 eikä häiritse työntekijöitä. Lisäksi päädyimme siihen, että nämä ohjelmistot joita tulemme vertailemaan, ovat jo ennestään tuttuja meidän yritykselle jolloin niiden asennus ja konfigurointi ei vaadi lisäopiskelua it-tiimiltä.

Valitsimme vertailtavaksi kolme tietoturvaohjelmistoa jotka täyttivät yllä mainitut kriteerit. Nämä ohjelmat olivat F-Securen Client Security 10.00, Windowsin oma Security Essential joka on Windows 8-käyttöjärjestelmässä nimellä Windows Defender ja Symantec Endpoint Protection. Seuraavaksi käydään läpi ohjelmistojen tärkeimmät ominaisuudet, plussat ja miinukset.

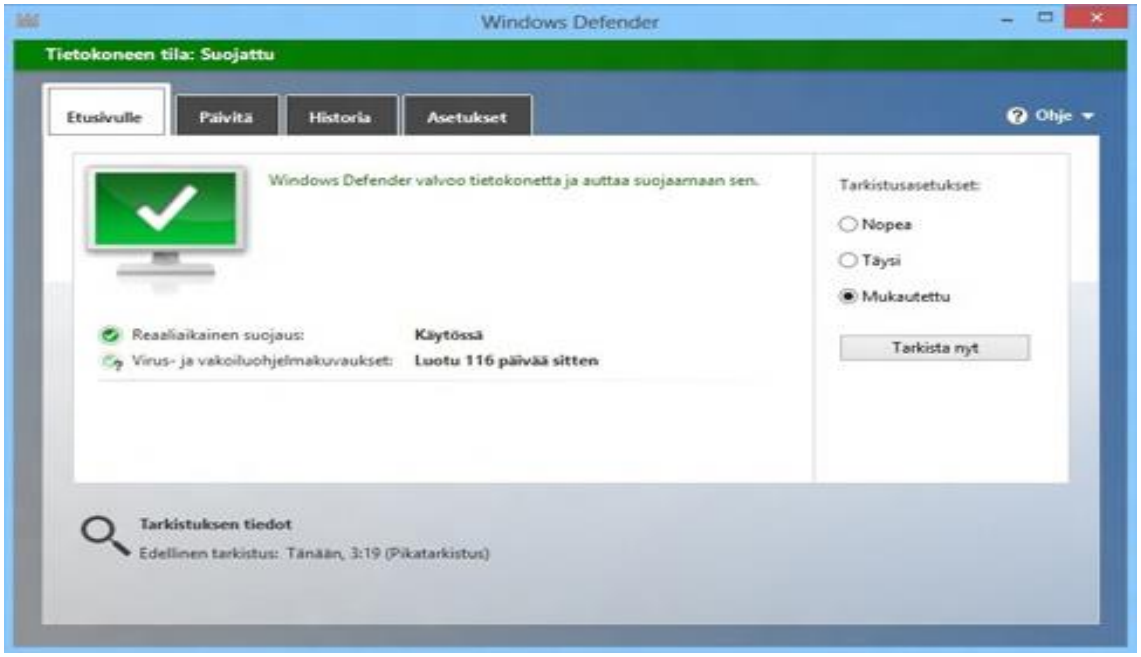
4.1 Ohjelmien tarkastelu

F-Securen Client Security 10.00 on tarkoitettu yrityksille jotka haluavat keskitetysti hallita työasemien tietoturvaa jolloin päivityksistä huolehtii yrityksen it-osasto. Kyseinen ohjelmisto sisältää oman palomuurin joten Windowsin palomuuri kytketään pois päältä Client Securityn asennusvaiheessa automaattisesti. Monet Client Securityn aiemmat versiot ovat useimmiten sijoittuneet tietoturvaohjelmistojen testeissä kärkikolmikkoon. Sen haittaohjelmien havaitsemiskyky on AV-Test sivuston mukaan yksi parhaimmista. AV-Test sivu on puolueeton ja itsenäinen instituutti joka testaa joka kuukausi virustorjuntaohjelmistoja ja luo niistä raportteja. (AV-Test, 2013)



Kuva 2. F-Secure Client Securityn aloitusnäkymä.

Windows Defender on Microsoftin oma tietoturvaohjelmisto joka tulee Windows 8 mukana. Se pohjana on käytetty Security Essentialsia jonka pystyi asentamaan Windows 7-koneelle halutessaan. Ohjelmaa ei pysty poistamaan koneeltaan, mutta se kytkeytyy pois päältä automaattisesti, kun asennetaan kolmannen osapuolen virustorjuntaohjelmisto.



Kuva 3. Windows Defenderin aloitusnäkymä.

Symantec Endpoint Protection kuvassa 4 on yrityskäyttöön tarkoitettu virustorjuntaohjelmisto. Ohjelmistoa voi käyttää sekä työasemiin että palvelimiin. Käyttöjärjestelmien valikoima, mihin voi asentaa, on todella laaja. Symantec-yritys on eräs suurimmista ja vanhimmista tietoturvayrityksistä, mikä näkyy ohjelmiston toimivuudessa. Se on sekä nopea että helppokäyttöinen. Huono puoli ohjelmistossa on se että sitä ei saa suomenkielisenä.

Kuva 4. Symantec Endpoint Protection alkuvalikko.

4.2 Tuotteen valinta

Taulukossa 1 näkyy tiedot vertailtavista kohteista jossa otettiin huomioon ohjelmien hyvät ja huonot puolet. Kriteereinä käytettiin asioita jotka olivat Agenteqille tärkeitä ja jotka ratkaisisivat mitä ohjelmistoa tullaan käyttämään.

Taulukko 1. Ohjelmistojen vertailutaulukko.

F-Secure Client Security	Windows Defender	Symantec Endpoint Protection
+Suomalainen +Havaitsemiskyky +Keskitetty hallinta +Yritykselle tuttu +Hyvä tuki	+Ilmainen +Asennettu valmiiksi +Aktiivinen taustasuojaus	+Havaitsemiskyky +Keskitetty hallinta +Helppokäyttöisyys
-Maksullinen -Suorituskyky -Ohjelman monimutkaisuus	-Havaitsemiskyky -Ei keskitettyä hallintaa -Suojaus	-Ei suomenkielinen -Tukipalvelut englanniksi -Maksullinen

Suurin painoarvo oli sillä että ohjelmiston haittaohjelmien havaitseminen olisi markkinoiden parhaimpia. Lisäksi sitä pitäisi pystyä hallitsemaan keskitetysti ja automatisoimaan. Päädyimme ottamaan käyttöön F-Securen Client Securityn. Agenteq oli jo jonkin aikaa käyttänyt Client Securityn versiota 9.20 joka oli toiminut moitteetta eikä sen kanssa oltu havaittu mitään ongelmia työasemissa. Itselläni oli myös koulutusta keskitetyn hallintaohjelmiston Policy Managerin käytössä joten sen ottaminen käyttöön oli kustannustehokasta, koska ei tarvinnut erillistä konsulttia tilata ohjelmiston konfigurointiin ja asennukseen. Lisäksi siihen vaikutti myös se että kyseessä oli suomalainen tuote hyvällä tukipalvelulla josta saa nopeaa tukea ongelmatilanteissa. Nämä edellä mainitut asiat johtivat päätökseen alkaa käyttämään F-Securen tuotetta.

5 KOLMANNEN OSAPUOLEN OHJELMISTOJEN PÄIVITYKSEN AUTOMATISOINTI

Nykyään yleisin hyökkäys työasemiin tehdään selaimen kautta. Niissä aina käytetään jonkin softan tai pluginin haavoittuvuutta kuten Javaa tai Adobe flashia. Tämä johtuu siitä, että useimmiten käyttäjät unohtavat päivittää näitä ohjelmistoja tai ovat liian kiireisiä huomaamaan että ohjelmasta on olemassa uudempi versio. (F-Secure, 2013) Useimmissa ohjelmissa on myös se huono puoli että ne eivät ilmoita jos uusia päivityksiä löytyy niihin jolloin käyttäjä joutuu itse manuaalisesti tarkistamaan ohjelmien kotisivuilta onko uutta versiota ladattavissa.

Kolmannen osapuolen ohjelmistojen päivitykseen löytyy laaja kirjo kansainvälisiä ohjelmia jotka joko toimivat itsenäisesti tai WSUS:n eli Microsoft Windows Server Update Servicen kanssa. Niistä jotkut sisältävät toiminnallisuuksia kuten raportointia tai keskitettyä hallintaa.

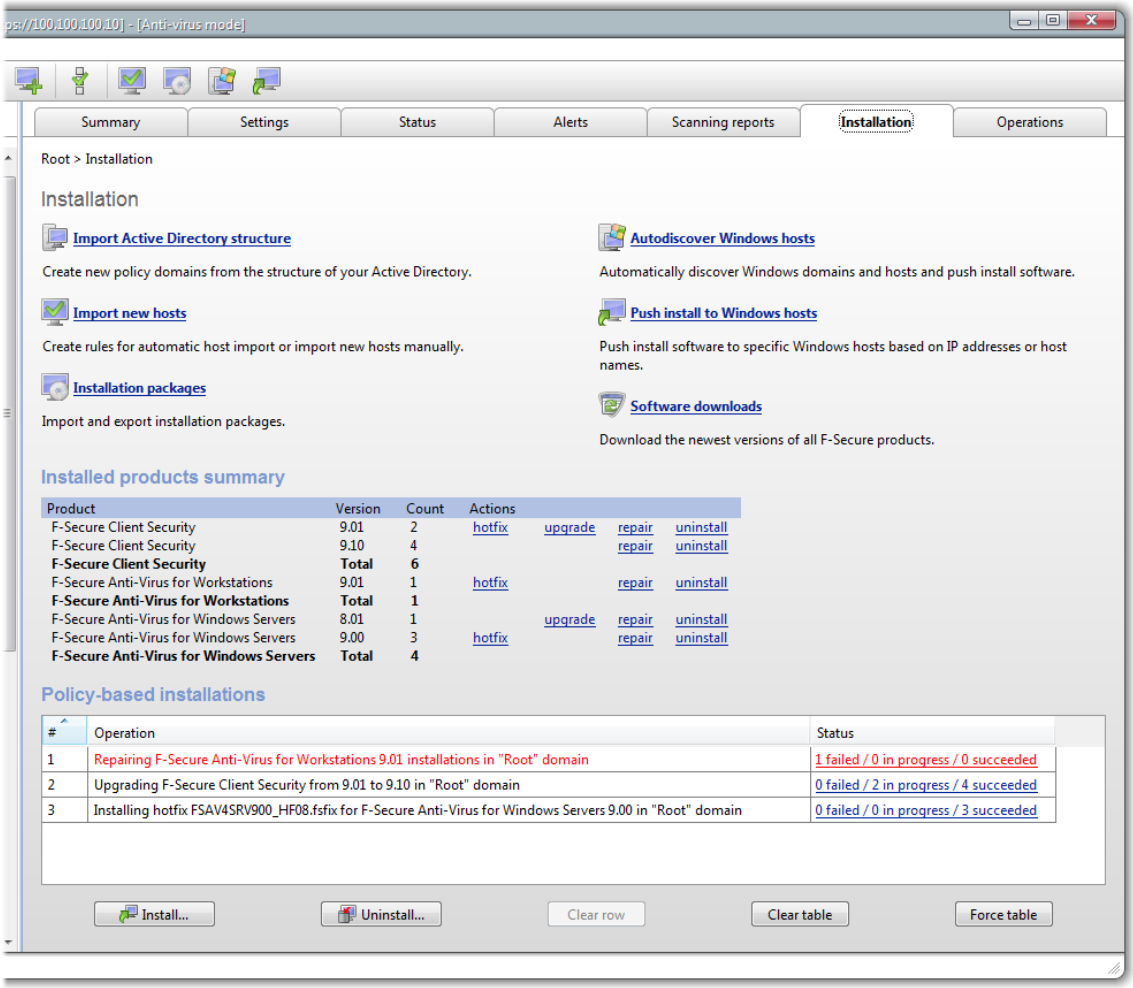
Agenteqille halusimme ohjelman jota pystyy etänä hallitsemaan jolloin yrityksen työntekijöiden ei tarvitse käyttää omaa työaikaa ohjelmistojen päivittämiseen. Otimme testattavaksi ja vertailtavaksi kaksi ohjelmaa jotka täyttivät kokonaan tai osittain haluamamme toiminnallisuudet. Nämä olivat F-Securen Client Securityn mukana tullut lisäosa Updater ja Microsoftin WSUS.

5.1 Kolmannen osapuolen sovellusten päivitysohjelmistot

F-Securen Updater sisältyy uusimman Client Security 10:n kanssa jos ottaa käyttöön Business Suite Premiumin. Sitä pystyy hallinnoimaan keskitetysti Policy Managerilla. Sillä saa päivitettyä sekä 3. osapuolen sovellukset että Windowsin omat käyttöjärjestelmäpäivitykset. Tämä on maksullinen lisäosa joka ei sisälly normaaliin Client Securityyn.

Policy Manager käyttöliittymässä kuvassa 5 voi valita minkä tyyppisiä päivityksiä asennetaan mihinkin työasemaan. Yleensä yrityksissä ei haluta kaikki päivityksiä asentaa, koska ne voivat joko rikkoa käyttöjärjestelmän tai sitten yrityk-

sessä tarvitaan tiettyä versiota esimerkiksi Javasta jolloin päivityksen asentaminen ei ole suotavaa. (F-Secure, 2013)

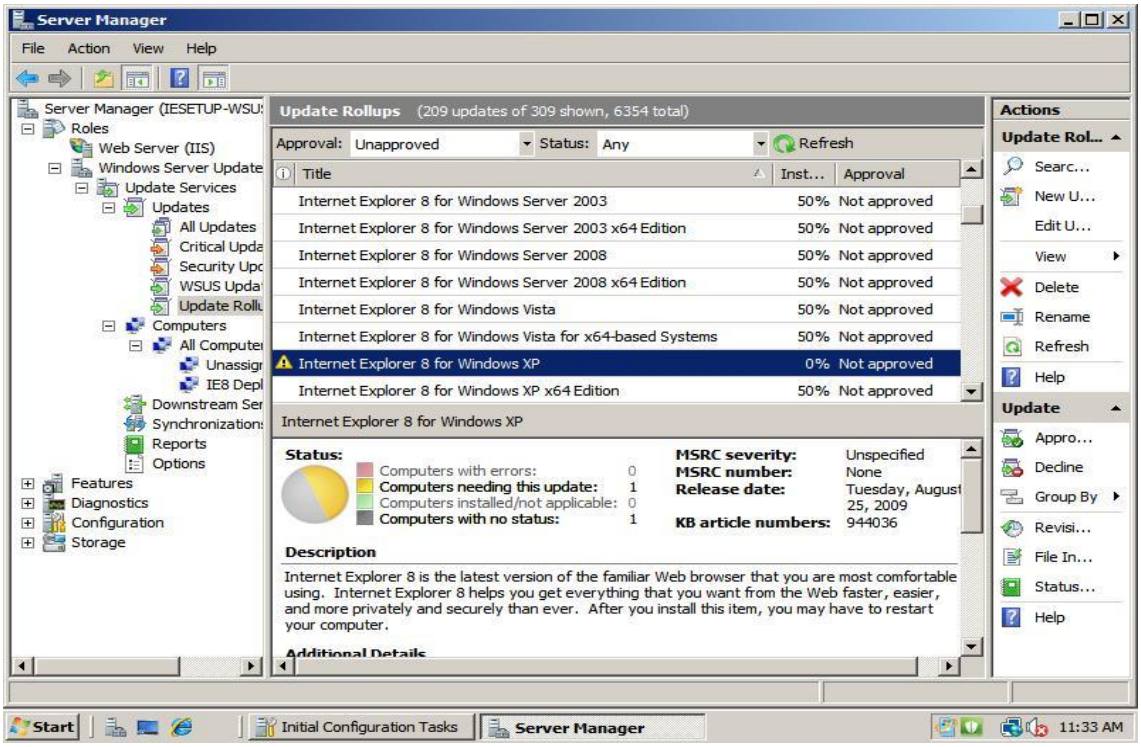


Kuva 5. Policy Managerin päivitysnäkymä.

Microsoft WSUS:a joka näkyy kuvassa 6, käytetään jakamaan automaattisesti Microsoftin omia päivityksiä käyttöjärjestelmiin. Palvelimen pystyy ajastamaan jolloin ei tarvitse järjestelmänvalvojan erikseen käydä ohjelmaa käynnistämässä. Aluksi uudet päivitykset haetaan Windowsin päivityspalvelimilta jonka jälkeen ne ovat valmiita jaettavaksi yrityksen sisäverkon työasemiin ja palvelimiin. (MikroPC, 2005)

Kolmansien osapuolen sovellusten päivitys on WSUS:n kanssa hankalampaa kuin Windows päivitysten asennus. Se vaatii erinäköisiä konfigurointeja Active Directoryn group policeihin. Järjestelmän valvojan halutessa päivittää tietyn so-

velluksen hänen täytyy aluksi hakea se asennusohjelma ja paketoida se WSUS:a varten ja vasta tämän jälkeen sen voi jakaa työasemille. (WindowsIT-Pro, 2011)



Kuva 6. WSUS hallintapaneeli

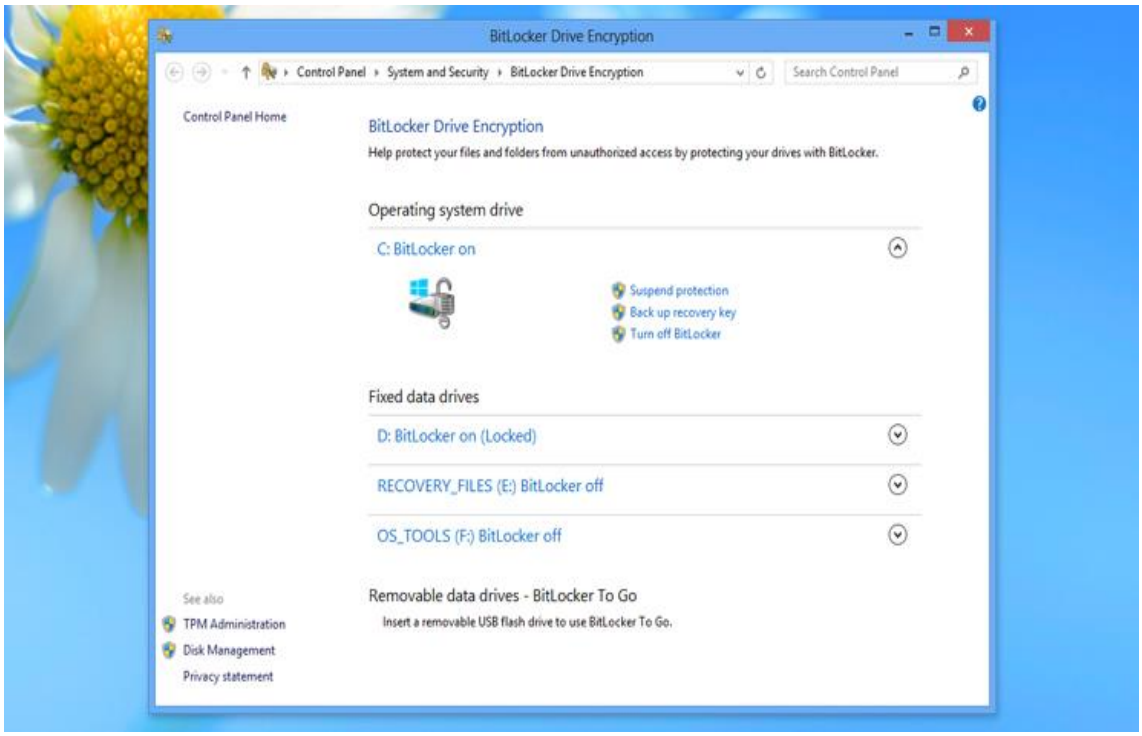
5.2 Ohjelmiston valinta

Sekä minä että IT-päällikkö käytiin F-Securen tilaisuuksissa kuuntelemassa miltä tuote vaikuttaa ja miten sitä käytetään. Olimme molemmat samaa mieltä siitä että otamme heidän tuotteen käyttöön, koska olemme jo päättäneet käyttää F-Securen Client Securitya Policy Managerin kanssa jolloin myös Updaterin käyttö olisi järkevää. Näiden kolmen yhdistelmä nostaisi Agenteqin tietoturvataso korkeammalle mitä se nyt on. F-Securen tuote sopii myös Agenteqille, koska yritys tarvitsee tuotteen joka tuottaa helppolukuisia raportteja ja pystyy automatisoimaan melkein kaikki toiminnot. Lisäksi halusimme käyttää suomalaista tuotetta jonka tuki on asiantuntevaa ja nopeaa. WSUS tarjosi ainoastaan osan meillä tarvituista toiminnoista. F-Securen tuotteiden käyttöönotto ja konfigurointi

on minulle myös helpompaa, koska olen työskennellyt yrityksen tuessa ja saanut arvokasta kokemusta heidän tuotteidensa käytöstä.

6 KOVALEVYJEN SALAUS

Työasemien kryptaukseen käytetään Windowsin omaa levynsalausohjelmaa Bitlockeria. Tämä päätös tehtiin yhteisymmärryksessä it-päällikön kanssa, koska kyseinen ohjelmisto on yhteensopivin Windows-työasemien kanssa jolloin vältytään ongelmatilanteilta. Kyseessä on kuitenkin yritys jonka kaikki työasemat ovat Windows-koneita joten mielellään käytetään Microsoftin omia tuotteita.



Kuva 7. Bitlockerin valikko Windows 8-työasemalla.

Bitlocker joka näkyy kuvassa 7 on kiintolevyjen ja muistilaitteiden kuten usb-muistitikun salausohjelma, joka sisältyy Windows Vistan ja Windows 7:n Enterprise- ja Ultimate-versioihin sekä Windows 8:n Pro- ja Enterprise-versioihin. Sen ollessa päällä se kysyy asetettua salasanaa ennen levyjen salauksen avaamista. Salaamisen voi asettaa myös siten, että tiedostot aukeavat vain, kun tietty laite on kytketty tietokoneeseen tai sitten se voidaan avata käyttäen avainta jonka saa tallennettua tekstitiedostoon. (Wikipedia, 2013)

Bitlockerilla voidaan salata joko yksittäinen osio, kokonainen kiintolevy tai sitten useita erillisiä levyjä. Kryptaamiseen eli salaamiseen käytetään AES(Advanced encryption stantard) salausta joka käyttää 128-bittistä salausavainta. AES on lohkosalausmenetelmä eli se salaa tietyn mittaisen dataosion kerrallaan. (Wikipedia, 2013)

Otin käyttöön Bitlockerin ainoastaan koneissa joissa on Windows 8 tai uudempi käyttöjärjestelmä. Tämä johtuu siitä että Agenteqilla Solutionsilla ei ole työasemissa käytössä Windows 7 Enterprise- tai Ultimate-versioita joiden mukana Bitlocker-ohjelma tulee. Tämän takia otin käyttöön vanhemmissa käyttöjärjestelmissä avoimen lähdekoodiin perustuvan Truecrypt-levynsalausohjelmiston. Sen toimintaperiaatteet ovat samat kuin Bitlockerilla.

Jokainen levyosio salataan ja niiden palautusavaimet tallennetaan verkossa olevaan verkkopalvelimelle johon ainoastaan IT-tiimillä on oikeudet. Bitlockerin levyjen salaukseen ei aseteta erillistä salasanaa vaan siinä käytetään Windowsin omaa autentikaatiota ja kirjautuessa koneelle kaikki levyosioiden salaukset puretaan automaattisesti.

7 YRITYKSEN TYÖASEMAN TIETOTURVALLISET KOKOONPANOASETUKSET

Tämä kappale on salattu

8 YHTEENVETO

Tämän työn tavoitteena oli perehtyä tietoturvaohjelmistoihin ja vertailla mikä niistä sopisi Agenteqille ja Suomen Talokeskukselle jolla saataisiin yhtenäistettyä tietoturvakäytäntöjä työasemien kohdalla. Yritys halusi ratkaisun jolla pystyi ylläpitämään molempien yritysten työasemia. Lisäksi pyrittiin myös siihen, että tällä opinnäytetyöllä saadaan yrityksen tietoturvaa parannettua.

Jouduin aluksi aika paljon rajaamaan aihetta, koska siihen olisi voinut sisällyttää muitakin asioita kuten käyttöoikeudet, palomuuriasetukset . Tämä olisi voinut johtaa siihen että työstä tulee liian laaja eikä päästä aiheisiin syvällisemmin perehtymään. Tämän takia valitsin it-päällikön kanssa 3 aluetta työaseman tietoturvasta jotka tulevat olemaan tärkeimmät osa-alueet joihin keskitymme konsernin työasemissa.

Ohjelmistojen vertailu oli jonkin verran hankalaa, koska ohjelmistoja löytyi monenlaisia mutta tietoa niistä ei kauheasti mistään löytynyt. Ainoa vaihtoehto olisi ollut lähteä testaamaan kyseisiä ohjelmistoja, mutta se olisi vienyt turhan paljon aikaa. Lisäksi monilla ohjelmistoista ei ollut trial-versiota jota olisi voinut käyttää tietyn ajan. Näiden syiden takia emme vertailleet kuin muutamaa ohjelmaa jotka olivat jo ennestään tuttuja yrityksessämme.

Työtä tehdessäni ymmärsin paremmin kuinka tärkeää on pitää ohjelmistot päivitettynä ja kuinka raskaaksi se tulisi jos työasemia joutuisi manuaalisesti päivittelemään kone kerrallaan. Opin arvostamaan yritysten kehittämiä hallintaohjelmistoja jotka helpottavat minun ja muiden järjestelmäylläpitäjien työtä. Sain myös todella arvokasta kokemusta tulevaisuutta ajatellen, koska tietoturva on eräs nopeinten kasvavista osa-alueista IT-alalla.

LÄHTEET

Agenteq. 2013. Kotisivut. Viitattu 21.8.2013 http://www.agenteq.fi/lyhyesti/

AV-Test. 2013. Yritysratkaisut, Windows 8. Viitattu 7.10.2013 http://www.av-test.org/en/tests/corporate-user/windows-8/janfeb-2013/

Finder. 2013. Taloustiedot. Viitattu 21.8.2013 http://www.finder.fi/ITsovelluksia,%20ITohjelmistoja/Agenteq%20Solutions%20Oy/SALO/taloustiedot/1171477/

F-Secure. 2013a. Software Updater. Viitattu 17.10.2013 http://www.f-secure.com/fi/web/business_fi/software-updater

F-Secure. 2013b. Software Updater. Viitattu 17.10.2013 http://www.f-secure.com/en/c/document_library/get_file?uuid=65e7a77b-f083-416e-b778-ac6fea7c9c85&groupId=30743

Hakala; Vainio; Vuorio, P. 2006. Tietoturvallisuuden käsikirja. 1. painos. Porvoo: Docendo

MikroPC. 2005. WSUS. Viitattu 17.10.2013 http://mpc.fi/nettilehti/pdf/1808200514.pdf

Ruohonen, M. 2002. Tietoturva. Jyväskylä: Docendo

Suomen internetopas. 2013. Viitattu 22.10.2013 http://www.internetopas.com/yleistietoa/tietoturva/

Tietoturvapalvelu. 2013. Viitattu 4.9.2013 http://www.tietoturvapalvelu.info/johdanto/haittaohjelmat_ja_muut_uhat

Vahti. 3/2004. Haittaohjelmista suojautumisen yleisohje. Viitattu 4.9.2013 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/88078_fi.pdf

Wikipedia. 2013. AES. Viitattu 18.10.2013 http://fi.wikipedia.org/wiki/BitLocker

Wikipedia. 2013. Bitlocker. Viitattu 14.10.2013 http://fi.wikipedia.org/wiki/BitLocker

Wikipedia. 2013. Rootkit. Viitattu 11.11.2013 http://fi.wikipedia.org/wiki/Rootkit

Wikipedia. 2013. Tietoturva. Viitattu 22.7.2013 http://fi.wikipedia.org/wiki/tietoturva

Wikipedia. 2013. Työasema. Viitattu 31.7.2013 http://fi.wikipedia.org/wiki/Työasema

WindowsITPro. 2013. Publishing Third-Party Updates to WSUS. Viitattu 17.10.2013 http://windowsitpro.com/systems-management/publishing-third-party-updates-wsus