

Microsoftin ja F-Securen päivitysten keskitetty hallinta työasemissa
Central management of Microsoft and F-Secure updates in work-
stations

Eero Teräs a0703502

Lopullinenversio

Seminaari 4.10.2010. Opponentit Sauli Jurmu ja Henna Lamminen



Tradenomi

Tekijät Eero Teräs	Ryhmä IM07TK
Opinnäytetyön nimi Microsoftin ja F-Securen päivitysten keskitetty hallinta työasemissa	28
Ohjaajat Tiina Koskelainen	
<p>Projekti tehtiin Valtion Taidemuseolle ja siinä otettiin käyttöön kaksi työasemien tietoturvaan parantavaa palvelua. Ensimmäinen niistä on Microsoft WSUS-palvelu, jonka avulla työasemien käyttöjärjestelmäpäivitykset saadaan pidettyä ajan tasalla. Toinen on F-Secure Policy Manager -palvelu, jonka avulla voidaan hallita keskitetysti työasemissa olevaa tietoturvaohjelmistoa.</p> <p>Näiden palveluiden katsottiin olevan ensisijaisen tärkeitä työasemien tietoturvan parantamiseksi. Ennen palveluiden käyttöönottoa työasemien Windows-käyttöjärjestelmiä ei ole päivitetty käyttöönoton jälkeen.</p> <p>Työasemissa oli aiemmin käytössä F-Secure Anti-Virus-ohjelmisto, joka suojasi työasemia puutteellisesti, ja hidasti virustietokantapäivitys-skriptin takia kirjautumista.</p> <p>Projekti koostui suunnitelmasta, testauksesta ja toteutuksesta. Suunnitelmassa määritettiin projektin eteneminen. Testausvaiheessa kokeiltiin päivitysten jakamista testiympäristössä, sekä tietoturvaohjelmiston keskitettyä hallintaa. Toteutusvaiheessa palvelut asennettiin tuotantopalvelimelle ja palvelut otettiin käyttöön kaikissa Windows-työasemissa, joita on noin 250 kappaletta.</p> <p>Projektin lopputuloksena syntyi kaksi palvelua, jotka paransivat tietoturvaan huomattavasti. Virhetilanteita silmälläpitäen työasemien sijainnit kartoitettiin etukäteen ja niiden nimet muutettiin yhteneväisiksi. Uuden enemmän resursseja syövän haittaohjelmientorjuntaohjelmiston ei haluttu hidastavan käyttäjien työntekoa, joten moneen työasemaan lisättiin keskusmuistia ja vanhimpia vaihdettiin uusiin.</p>	
Asiasanat järjestelmänhallinta, tietoturva, päivitys	

Tradenomi

<p>Authors Eero Teräs</p>	<p>Group IM07TK</p>
<p>The title of thesis Central management of Microsoft and F-Secure updates in workstations</p>	<p>28</p>
<p>Supervisors Tiina Koskelainen</p>	
<p>The project was commissioned by the Finnish National Gallery. It deals with taking into use two services to improve workstation security. The first service is Microsoft WSUS -service, which allows desktop operating system updates to be kept up to date. Another service is F-Secure Policy Manager Service, which is used to centrally manage security software on the workstations.</p> <p>These services are considered to be of primary importance when improving security. Before these services Windows operating systems were not updated after the initial installation.</p> <p>The workstations used to have F-Secure Anti-Virus software, which did not protect the workstations very well. The virus database update script also slowed down the computers.</p> <p>The project consisted of designing, testing and the implementation of the services. The design of the requirements determined the outcome of the project. In the testing phase a trial was run in the test environment, of sharing updates and security software for centralized management. In the implementation phase the services were installed in the production server and (services were installed) in all of the Windows-based workstations.</p> <p>The project resulted is two services, which improved security considerably. At the same time the locations of the workstations were mapped and the names of the desktop computers were changed to be convergent. Also the processor speed and memory of the workstation were reported.</p>	
<p>Key words system management, security, updates</p>	

Sisällys

1 Johdanto	1
2 Ohjelmistojen päivittämisen tarve	3
2.1 Tausta ohjelmistojen ja laitteiden synnylle	3
2.2 Päivitysten tarve ja tietoturva	7
2.3 Nykyaikaiset päivitystavat	9
2.3.1 SCCM (System Center Configuration Manager 2007)	9
2.3.2 Automaattiset päivitykset suoraan Microsoftilta	10
2.3.3 WSUS (Windows Server Update Services)	11
2.4 F-Securen päivittäminen	17
3 Ohjelmistojen keskitetty päivittäminen Valtion Taidemuseossa	18
3.1 Taustaa	19
3.2 Lähtötilanne	20
3.3 Suunnitelma	22
3.4 Toteutus	23
3.4.1 Testiympäristö	23
3.4.2 F-Secure Policy Manager	23
3.4.3 WSUS-palvelu	25
3.5 Tulokset	29
3.5.1 F-Secure Policy Manager	29
3.5.2 WSUS-palvelu	30
4 Tulosten tarkastelu	30
4.1 Projektin vaikutukset	31
4.2 Projektin haasteita	32
4.3 Oma oppiminen	32
4.4 Ideoita ja jatkokehitystä	33
Lähteet	35
Liitteet	39
Liite 1. Projektisuunnitelma	39

1 Johdanto

Tässä raportissa käsitellään Microsoftin ja F-Securen -ohjelmistojen keskitettyä hallintaa ja niiden käyttöä yleisesti sekä erityisesti Valtion Taidemuseon tietohallinnossa.

Tavoitteena oli luoda työasemien keskitetty hallinta, käyttöjärjestelmän päivitysten ja tietoturvaohjelmiston osalta. Näillä palveluilla saataisiin tietoturvaa parannettua merkittävästi. Erityisen tärkeänä pidettiin Windows XP-käyttöjärjestelmän tietoturvapäivitysten seuranta ja asentamista, koska Windows XP-käyttöjärjestelmä on suurimassa osassa työasemista. Vanhan F-Secure Anti-Virus (versio 5.xx)-ohjelmiston vaihtamista monipuolisempaan ja uudempaan tuotteeseen, pidettiin myös tärkeänä tavoitteena. Uutta tietoturvaohjelmistoa tulisi pystyä myös hallitsemaan keskitetysti. Tietoturvaohjelmiston keskitetyn hallinnan avulla tulisi pystyä lähettämään uudet asetukset työasemissa oleviin tietoturvaohjelmistoihin. Ilmoitukset tulee saada saastuneista tiedostoista ja työasemista, sekä siitä jos työaseman tietoturvaohjelmiston virustunnistetietokanta ei päivity. Uuden version lähettäminen tietoturvaohjelmistosta pitäisi myös onnistua.

Mahdollisia ongelmia Windows-ympäristössä ajateltiin aiheuttavan aktiivihakemiston puute sekä työasemissa olevien ohjelmien mahdolliset ristiriidat. Tietokoneiden suorituskyvyn puute voisi myös aiheuttaa ongelmia, jos uusi tietoturvaohjelmisto hidastaisi liikaa työaseman käyttöä. Työasemien nimeämisestä oli vuosien saatossa monta eri versiota, mikä aiheuttaa ongelmia työasemien sijainnin selvittämisessä. Työaseman sijainnista ollaan kiinnostuneita virhetilanteissa, jotka edellyttävät toimenpiteitä suoraan työasemalla.

Opinnäytetyö on rajattu niin, että tietoturvassa keskitytään vain ohjelmistoturvallisuuden ja siinä vain F-Securen ja Microsoftin tuotteiden osalta. Käyttöjärjestelmien kohdalla keskitytään vain Microsoft Windowsiin. Valtion Taidemuseossa on myös useita Mac-työasemia ja muutama Linux-työasema, mutta niihin ei virallisesti anneta käyttöä, vaan käyttäjien tulee itse huolehtia niistä ja ratkoa mahdolliset ongelmat. Käytännössä Mac- ja Linux-tietokoneille annetaan kuitenkin teknistä tukea tarvittaessa mahdollisuuksien mukaan.

WSUS-palvelusta (Windows Server Update Services, ks. kappale 2.3.3 WSUS) voi jakaa päivityksiä melko moneen Microsoft-tuotteeseen, tässä opinnäytetyössä kuitenkin keskitytään Windows XP:seen. Muihin Microsoftin tuotteisiin päivitysten jakelu onnistuu samaan tapaan. Valtion Taidemuseon työasemia ei ole liitetty aktiivihakemistoon (Active Directory, Ad), joten sitä ei käsitellä.

Tässä opinnäytetyössä käytettyjä käsitteitä ovat:

Tietoturvaohjelmisto = Ohjelma tai ohjelmakokonaisuus, jolla työaseman saastumista pyritään estämään

Aktiivihakemisto = (Active directory, Ad) on hakemistopalvelu joka perustuu Internet-standardeihin. Yleisimmät käyttökohteet ovat käyttäjien ja työasemien tietojenhallinta. Eri palvelut voivat hakea tiedot keskitetysti yhdestä paikasta. Aktiivihakemisto on siis tietokannan tapainen tietovarasto

WSUS-palvelu = Windows Server Update Services on Microsoftin tuotteiden keskitettyyn päivittämiseen tarkoitettu palvelinohjelmisto

Novell Client = Novell-asiakasohjelma on työasemaohjelmisto, joka tuo helppokäyttöisen, turvattun ja hallittavan verkkoympäristön käyttäjilleen. Se mahdollistaa käyttäjän pääsyn NetWare-palveluihin työasemilta tai palvelimilta. Sillä voi esimerkiksi selata NetWare hakemistoja, siirtää tiedostoja, tulostaa asiakirjoja ja voi käyttää kehittyneitä NetWare-palveluita suoraan työasemalta

SCCM = Tulee sanoista System Center Configuration Manager. Se on Microsoftin järjestelmänhallinta työkalu. Sillä hallitaan keskitetysti laajoja Windows-ympäristöjä. Ylläpitäjät voivat tällä asentaa sovelluksia ja päivittää järjestelmiä

takaovi = Mahdollistaa tietokoneelle luvattoman pääsyn ulkopuoliselle henkilölle verkon välityksellä.

Rootkit = ohjelmisto, joka mahdollistaa jatkuvan etuoikeutetun pääsyn tietokoneelle. Se piilottaa itseään aktiivisesti järjestelmänvalvojalta turmelemalla järjestelmän vakio toiminnallisuuksia tai muita ohjelmia.

Troijalainen = on ohjelma joka näyttää suorittavan toivottua tehtävää, mutta se varastaa tietoa tai vahingoittaa järjestelmää

Windowsin Automaattiset päivitykset = (Windows Update) on palvelu, jolla Microsoft tarjoaa päivityksiä Windows-käyttöjärjestelmälle ja sen osille, mukaan lukien Internet Exploreriin. Laajennettu versio tästä palvelusta tarjoaa päivitykset myös muille Microsoftin tuotteille kuten Office, Windows Live ja Microsoft Expression Studio. Päivitykset yleensä tarjotaan internet-yhteyden kautta

2 Ohjelmistojen päivittämisen tarve

Ohjelmistoja päivitetään useasta eri syystä. Ohjelmistojen tietoturva haavoittuvuuksien takia on ohjelmisto syytä päivittää, esimerkiksi SQL-injektion mahdollisuus on tällainen. Päivitystarve voi myös seurata siitä, että ohjelmisto ei toimi odotetulla/toivotulla tavalla esimerkiksi ohjelma laskee väärin tai ei ole tarpeeksi tehokas tai nopea. Päivitys voi olla paikallaan kun ohjelmistopäivitys tarjoaa uuden ominaisuuden tai toiminnallisuuden joka halutaan ottaa käyttöön esimerkiksi käyttöliittymä ruotsinkielellä. Joidenkin ohjelmien tehokas toiminta vaatii ajantasaista tietoa esimerkiksi virustietokantojen uusi versio. Yleisesti ottaen ohjelmointivirheet luokitellaan syntaksivirheisiin ja semanttisiin virheisiin (Jyväskylän yliopisto Tietotekniikan laitos 2011).

2.1 Tausta ohjelmistojen ja laitteiden synnylle

Tarve päivittämiselle on lisääntynyt räjähdysmäisesti tietokoneiden yleistymisen myötä. Ihmisten ja yhteiskunnan tarpeet toimivat kannustimena yhä uusien innovaatioiden, myös uusien teknologioiden kehittämiseksi. Eri toimijoiden välinen, erityisesti taloudellinen kilpailu vauhdittaa uusien ohjelmistotuotteiden kehittämistä. Viimeisten kahdenkymmenen vuoden aikana ohjelmistomarkkinat ovat kasvaneet räjähdysmäisesti.

Perusta ohjelmistomarkkinoiden kasvulle juontaa juurensa PC-tietokoneesta, Windowsin kehittymisestä, verkottumisesta, WWW-standardista ja Internet-selaimen kehittymisestä. Tietokoneiden verkottuminen alkoi ARPAnet-projektista vuonna 1967. Kahden tietokoneen välinen yhteys muodostettiin vuonna 1970 ja samana vuonna tietokoneita oli liitetty jo neljä kappaletta. IBM julkaisi 1981 henkilökohtaisen PC-tietokoneen. (Tie-

tokone 2006.). PC-tietokone menestyi markkinoilla ohjelmistotarjonnan ja avoimen arkkitehtuurin ansiosta. (Tietojenkäsittelytieteen laitos 2001.) Graafinen Windows-käyttöliittymä versio 3.0 julkaistiin vuonna 1990 (The Elder Geek on Windows XP 2010). Windowsin historia alkoi siitä, kun Applen Steven Jobs esitteli Microsoftin Bill Gatesille prototyyppiä Apple Lisa tietokoneesta vuonna 1981. Samana vuonna Microsoft alkoi kehittää graafista käyttöliittymää, jota kutsuttiin Interface Manageriksi, joka myöhemmin nimettiin Windowsiksi. Microsoft lupasi, että uusi tuote olisi saatavilla 1984. Windowsin ensimmäinen beta-versio ilmestyi 1983. Windows 1.0 julkaistiin 1985 lähes kaksi vuotta myöhässä alun perin luvatussa aikataulusta. (About.com 2010).

Käyttöjärjestelmät olivat aikaisemmin komentorivipohjaisia. Ne ovat hankalia kokemattomalle käyttäjälle, koska niiden käyttö vaatii monien komentojen ulkoa opettelua. Käyttöjärjestelmään kehitettiin graafinen käyttöliittymä helpottamaan käyttöä.

World Wide Web –standardin julkaisi CERN vuonna 1991. Erwise oli vuonna 1991 ensimmäinen graafinen Internet-selain. Erwisen tekivät kolme suomalaista insinööriä Kim Nyberg, Kari Sydänmaanlakka ja Teemu Rantanen. Erwise oli suunniteltu toimimaan X Window järjestelmässä. (Xconomy 2009.) Internet Explorer 1.0 julkaistiin vuonna 1995, joka oli sisällytetty Windows 95 käyttöjärjestelmään. (Microsoft 2003.) Ensimmäinen tavalliselle kuluttajalle suunnattu graafinen Internet-selain Mosaic-yhtiö julkaisi vuonna 1993.

Verkottuneet tietokoneet lisäävät tarvetta tietoturvapäivityksille, koska tietoverkossa haittaohjelmat leviävät paljon nopeammin, kuin aikaisemmin esimerkiksi levykkeiden välityksellä.

Ohjelmistomarkkinat kasvavat Suomessa noin 10 % vuodessa (Taulukko1). Alla olevassa taulukossa on kuvattu ohjelmistomarkkinoiden kasvua suomessa vuodesta 2004 vuoteen 2008. Tästä voi päätellä, että ohjelmistomarkkinoilla on voimakasta kasvua ja ettei kasvu ole pysähtymässä.

Taulukko 1. Ohjelmistoliiketoiminnan volyymi Suomessa

Vuosi	Ohjelmistoliiketoiminnan volyymi (Suomessa)	Kasvu
2004	1,65 Mrd €	
2005	1,82 Mrd €	10,2%
2006	1,95 Mrd €	7,8%
2007	2,14 Mrd €	9,2%
2008	2,32 Mrd €	8,7%

(Centre of Expertise for Ubiquitous Computing 2009)

Tietokoneita oli 1950-luvun lopussa noin 3000 kpl, 1960-luvun lopussa noin satatuhatta, vuonna 1994 mikrotietokoneita oli noin 48 miljoonaa (Turku Unix Users Group 1995), vuonna 2008 noin miljardi ja vuonna 2014 ennustetaan olevan kaksimiljardia kappaletta. Suurimmassa osassa tietokoneita on Windows-käyttöjärjestelmä. Vuonna 2009 Windows-käyttöjärjestelmiä oli 92 prosentissa tietokoneita. Siitä 18 prosenttia Vista, 4 prosenttia Windows 7 ja 69 prosenttia Windows XP –käyttöjärjestelmällä varustettuja tietokoneita (Computerworld 2009). Valtiovarainministeriön julkaisusta Tietoja valtion tietohallinnosta 2009 (Valtiovarainministeriö 2010.) ilmenee, että valtionhallinnon koneissa Windows on ylivoimainen (Taulukko2).

Taulukko 2. Valtion tietohallinnon käyttöjärjestelmien määrät 2008

Käyttöjärjestelmä	Henkilökohtaiset työasemat
Windows XP	85,6 %
Windows 2000 ja vanhemmat	2,2 %
Linux	3,1 %
MacOS	1,9 %
Windows Vista	5,1 %
Muu	0,4 %

(Valtiovarainministeriö 2010)

Haittaohjelmia on ohjelmoitu tietokoneisiin 1970 luvun alkupuoliskolta saakka. Tietomurtoja vuonna 2008 kirjattiin 285 miljoonaa. Tietomurron havaitsemiseen kestää viikkoja tai kuukausia 75 prosentista yrityksistä (Verizon 2009).

Vuonna 2009 uusia haittaohjelmia tuli ilmi noin 55000 päivässä (25 miljoonaa vuodessa). Niistä vain 6,6 % sisältää viruksia. Suurin osa eli 66 % on troijalaisia. Toiseksi eniten löytyi mainosohjelmia (eli adware:a), jotka myös luokitellaan haittaohjelmiksi (Tietokone 2010a). Huono tietoturva voi tulla yritykselle kalliiksi. Esimerkiksi Heartland-yhtiön järjestelmiin murtautuneilla rikollisilla oli pääsy 100 miljoonaan maksu- ja luotokortin tietoihin. Heartland-yhtiö joutui maksamaan Visalle ja muille yrityksille yli 60 miljoonan dollarin korvaukset, puutteellisesti hoidetun tietoturvan vuoksi (Tietokone 2010b).

Tätä taustaa vasten nousee henkilökohtaisten tietokoneiden ohjelmistojen markkinajohtajan Windowsin tietoturva erityisen keskeiseksi. Sen tietoturva on ollut – tai paremminkin sen tietoturvan puutteet ovat olleet keskeinen tekijä siinä, että virusten vastaiseen toimintaan on syntynyt kannattavat markkinat.

Suurimmat tietoturvaohjelmia tuottavat yritykset ovat Symantec, McAfee ja Trend Micro. Loput yritykset ovat kolmea markkinajohtajaa huomattavasti pienempiä.

Taulukko 3. Tietoturvaohjelmistoyritysten markkinatilanne. (Luvut ovat miljoonia dollareita. Vuosien 2009 ja 2010 tiedot ovat arvioita.)

Yritys	2004	2005	2006	2007	2008	2009	2010
Symantec	1915,3	2150,4	2564,3	2768,5	2968,7	-	-
McAfee	666,5	753,9	1072,9	1225,2	1475,7	-	-
Trend Micro	509,3	555,7	701,5	809,2	938,5	-	-
Muut	442,2	555,3	4356,2	6558,8	8096,6	-	-
Yhteensä	3533,2	4015,4	8694,9	11361,3	13479,7	≈14800	≈16500

(Gartner 2006, Gartner 2008, Gartner 2009)

Alla olevasta taulukosta voidaan havaita, että tietoturvaohjelmistoja tuottavat yritykset ovat Microsoftiin verrattaessakin kasvaneet suuriksi.

Taulukko 4. Microsoftin ja tietoturvayritysten liikevaihdon vertailu. (Luvut ovat miljoonia dollareita.)

	2004	2005	2006	2007	2008	2009	2010
Microsoft	36840,0	39790,0	44280,0	51120,0	60420,0	58440,0	62480,0
Kaikki tietotur- vayritykset	3533,2	4015,4	8694,9	11361,3	13479,7	14800	16500
Osuus Microsof- tin liikevaihdosta	9,6%	10,1%	19,6%	22,2%	22,3%	25,3%	26,4%

(Microsoft 2010)

2.2 Päivitysten tarve ja tietoturva

Haittaohjelmia torjumaan riitti aikaisemmin pelkkä virustorjuntaohjelma ja palomuuuri, mutta nykyään pitää suojautua myös madoilta, troijalaisilta, takaovi (backdoor), vakoi-
luohjelmilta, mainosohjelmilta ja rootkiteiltä.

Kun tietokoneohjelmia ja ohjelmistoja valmistetaan, niin ne käyvät läpi monta vaihetta, joilla pyritään varmistamaan, että ohjelma on valmis käytettäväksi ja myyntiin. Monesti viimeiset testiversiot annetaan rajoitetulle määrälle tavallisia käyttäjiä testattavaksi ennen tuotteen virallista julkistusta, tätä kutsutaan Beetatestaukseksi. Tällä tavalla pyritään löytämään tehokkaammin ohjelmistovirheitä. Esimerkiksi Microsoftin Windows XP käyttöjärjestelmästä julkaistiin viisi eri versiota ennen lopullista tuote julkistusta. (The Elder Geek on Windows XP 2010.)

Taulukko 5. Microsoft Windows XP:n versioiden julkaisuaikataulu

Ajankohta	Versio
Lokakuussa 2000	Windows Whistler Beta 1 (työnimellä)
Maaliskuussa 2001	Windows XP Beta 2
Kesäkuussa 2001	Windows XP RC 1 (Release Candidate versio kehittäjille)
Heinäkuussa 2001	Windows XP RC 2
Elokuussa 2001	Windows XP RTM (Release To Manufacturing versio laite valmistajille)
Lokakuussa 2001	Windows XP Home and Professional

(The Elder Geek on Windows XP 2010.)

Koska tuotteiden kehittämiseen kuluu paljon aikaa ja rahaa, on niiden saamiseksi lopputuotteen käyttäjälle suuria paineita. Vaikka eri testausvaiheissa löytyykin paljon ohjelmistovirheitä, ei niistä kaikkia pyritä korjaamaan ennen lopullista versiota. Uusia ohjelmistovirheitä löytyy koko tuotteen elinkaaren ajan. Tuotteen julkaisun jälkeen ohjelmistovirheitä paikkaavia päivityksiä julkaistaan säännöllisesti.

Vaikka ohjelmistotuotteissa on tietoturva otettu huomioon, niin ne ovat kuitenkin kaukana hyvästä tietoturvasta, koska korkea tietoturvataso myös hankaloittaa ohjelmistotuotteen käyttöä. Tämän takia monissa ohjelmistotuotteissa on oletuksena tietoturvataso melko matalalla. Esimerkiksi Windows XP:ssä on oletuksena autorun-toiminto käytössä, joka automaattisesti käynnistää cd-asemaan työnnetyn cd-levyn tai käynnistää elokuvan dvd-levyltä. Tämä toiminnallisuus on helposti todennettavissa, esimerkiksi laittamalla cd-levyn Windows XP -käyttöjärjestelmälliseen tietokoneen cd-asemaan. Huonona puolena tällaisella toiminnolla on se, että se käynnistää myös haittaohjelmat automaattisesti ja ne leviävät entistä nopeammin. Tämän tapaisilla käyttöä helpottavilla toiminnoilla on myös negatiiviset puolensa.

Haittaohjelmia on ollut melkein yhtä pitkään kuin tietokoneitakin ja tietokoneiden verkottuminen on mahdollistanut niiden nopean leviämisen. Koska kaikissa ohjelmissa on tietoturva-aukkoja, niin haittaohjelmien-tekijän kannattaa tehdä haittaohjelmia kaikkein

yleisimpiin ja turvattomimpiin. Microsoft on käyttöjärjestelmissä monopoliasemassa ja turvattomin, joten sen tuotteisiin tehdään eniten haittaohjelmia. Haittaohjelmat ovat myös luoneet ison markkinaraon tietoturvaohjelmistoille. G Data:n puolivuositaisesta haittaohjelmaraportista on havaittavissa, että haittaohjelmista 99 prosenttia tehdään Windows-käyttöjärjestelmille. Käyttöjärjestelmien suosiolla ja haittaohjelmien määrällä ei kuitenkaan näyttäisi olevan selvää yhteyttä. (G Data 2010, 6.)

Työaseman käyttöjärjestelmän ja sovellusohjelmien päivittäminen kuuluvat tietoturvan toiminnallisissa osa-alueissa ohjelmistoturvallisuuteen. Päivitykset auttavat poistamaan virhetilanteita ja paikkaavat tietoturva-aukkoja, joskus ne lisäävät myös ominaisuuksia, toiminnallisuutta, yhteensopivuutta tai parantavat suorituskykyä. Käyttöjärjestelmä ja ohjelmisto päivitykset tulisi testata ennen käyttöönottoa. (Tietoturvallisuuden käsikirja 2006, 11-12.)

Tietoturvaohjelmistoissa päivitetään ohjelmiston lisäksi sen tunnistetietokantaa, koska virus- ja haittaohjelmistojen torjunta perustuu siihen. Tietoturvaohjelmisto tunnistaa haittaohjelmat ja virukset vain, jos ne löytyvät tunnistetietokannasta. Tästä syystä tulisi tunnistetietokanta pitää ajan tasalla. Koska uusia viruksia ja haittaohjelmia ilmestyy nopeammin kuin tunnistetietokanta päivittyy, on ennakoivaan suojaukseen alettu kiinnittämään entistä enemmän huomiota. (Tietoturvallisuuden käsikirja 2006, 135-136.)

2.3 Nykyaikaiset päivitystavat

Microsoft Windows –käyttöjärjestelmän voi päivittää monella eri tavalla. Alla on mainittu niistä muutamia yleisempiä.

2.3.1 SCCM (System Center Configuration Manager 2007)

Vanhempi versio on SMS (Systems Management Server). SCCM on Microsoftin järjestelmä hallinta tuote, jolla voi keskitetysti hallita isoja ryhmiä Windows-pohjaisia tietokoneita.

SCCM tarjoaa etähallinnan, päivitysten hallinnan, ohjelmistojen jakelun, käyttöjärjestelmien jakelun, ja laitteisto- ja ohjelmistoinventaarion. Tämä tuote on tarkoitettu keski- ja suurille yrityksille.

2.3.2 Automaattiset päivitykset suoraan Microsoftilta

Windows-käyttöjärjestelmissä Automaattiset päivitykset tulee käyttöön suosituksena ja se lataa ja asentaa kaikki suositeltavat päivitykset joka päivä (kuvio 1).



Kuvio 1. Automaattiset päivitykset -välilehti

Automaattiset päivitykset –toiminto ottaa ajastetusti yhteyttä Microsoft Update - palveluun ja asentaa uusimmat päivitykset, jos niitä on saatavilla. Tämä **Automaattiset päivitykset** – toiminto on kätevä tapa pitää käyttöjärjestelmä ajan tasalla kotikäyttäjälle. Yritysten ei kuitenkaan kannata asentaa kaikkia Microsoftin suositettamia päivityksiä automaattisesti, koska kaikki päivityksiä ei ole testattu kohde järjestelmässä ja ne voivat aiheuttaa odottamattomia ongelmia.

2.3.3 WSUS (Windows Server Update Services)

Windows Software Update Services (WSUS), on Microsoftin ilmainen päivitystenhallintatyökalu. WSUS on uusi versio Microsoftin ilmaisesta päivitystenhallintatyökalusta, joka korvaa Software Update Services -palvelun tai lyhyemmin SUS-palvelun. WSUS tarjoaa useita uusia ominaisuuksia, kuten päivitysten kohdentamisen ennalta määritellyille ryhmille koneita, tukien useampaa Microsoftin tuotetta (esim. Office) ja parannetun raportoinnin.

WSUS-palvelua käytetään organisaation sisällä yhdellä tai useammalla palvelimella, jotta määritetään palvelemaan ohjelmistopäivitysten jakelua yhdelle tai useammalle asiakaskoneelle. WSUS-palvelun voi määrittää lataamaan päivityksiä joko Microsoftin tai muusta WSUS-palvelimesta organisaation sisällä. Kun olet hyväksynyt päivitykset asennettavaksi, WSUS-palvelu lataa sen määritettyä jakelukanavaa pitkin, ja voi sitten jakaa nämä päivitykset asiakaskoneelle joka niitä tarvitsee. Asiakaskoneille tai asiakaskone ryhmille voit hyväksyä minkä tahansa päivityksen, kaikki tai ei yhtään. Kun päivitys on hyväksytty, kohde WSUS-asiakkaalle ladataan päivitykset käyttäen Windows Automaattiset päivitykset -asiakasohjelmaa. WSUS-palvelu tarjoaa myös raportteja siitä mihin asiakaskoneeseen on mitäkin päivityksiä asennettu ja mitä niihin vielä voisi asentaa. (Windows Server Update Services Wiki 2010.)

WSUS-palvelu tarjoaa ominaisuuden, joka mahdollistaa Windows Automaattiset päivitykset -asiakasohjelman hankkia ja asentaa päivitykset. Kuitenkaan se ei tarjoa sisäistä versiota Windows päivitys -sivustosta, jolloin käyttäjät eivät voi navigoida WSUS-palvelussa ja hankkia päivityksiä (niin kuin he voivat, kun he käyttävät Microsoftin Windows Update-sivustoa). (Windows Server Update Services Wiki 2010.)

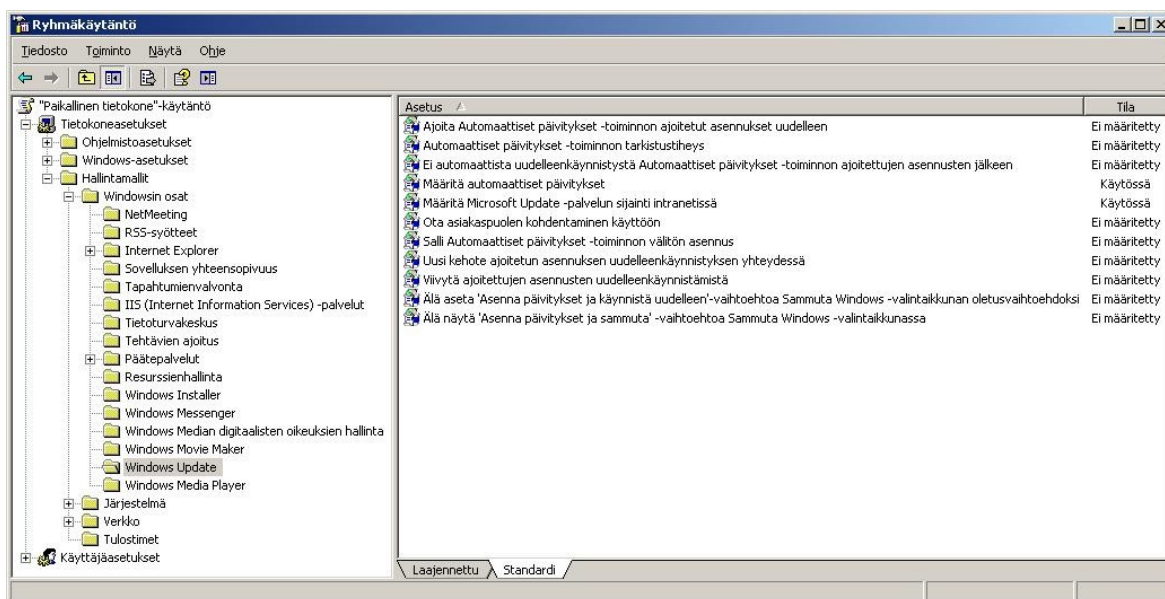
WSUS-palvelua voi hallinnoida hallintakonsolilla osoitteessa: <http://<WSUS-palvelimen nimi>:<portin numero>/WsusAdmin/>. WSUS-palvelimella voi myös Käynnistä Windows Server Update Services -ohjelman, joka löytyy Käynnistä-valikosta Hallintatyökalut-kohdasta. Huomaa, että jos et lisää WSUS-hallintakonsolin osoitetta

listaan paikallisista sivustoista Internet Exploreriin, niin näyttöön voi tulla kehote käyttöoikeuksista joka kerta, kun avaat WSUS-hallintakonsolin. (Windows Server Update Services Wiki 2010.)

WSUS-palvelu tukee myös mahdollisuutta sallia paikallisten järjestelmänvalvojen käyttää Automaattiset päivitykset -asiakasohjelmaa ohjauspaneelin kautta heidän valitsemilaan määrittämisellä. Huomaa että paikalliset järjestelmänvalvojat eivät voi poistaa automaattiset päivitykset -toimintoa pois käytöstä. Tämä asetus näkyy paikalliselle järjestelmänvalvojalle vain, jos automaattiset päivitykset -toiminto on päivittänyt itsensä versioon joka on yhteensopiva WSUS-palvelun kanssa. (Windows Server Update Services Wiki 2010.)

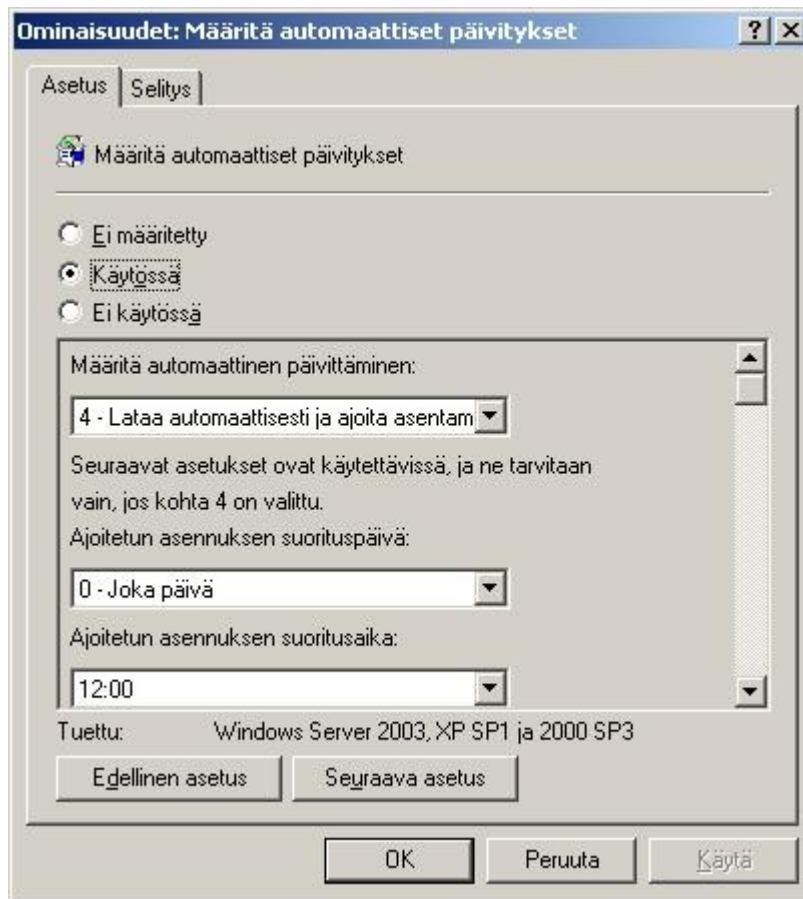
Tiedonsiirrossa käytetään BITS (Background Intelligent Transfer Service) taustalataustekniikkaa päivitysten lataamiseen Microsoftilta WSUS-palveluun, samalla tavalla kuin WSUS-palvelusta asiakaskoneille. BITS tukee myös tiedostojen lähetystä samaan toimialueeseen kuuluvien tietokoneiden välillä (Microsoft 2010d, 97).

WSUS-asiakaskoneelle täytyy tehdä vähintään seuraavat määrittäykset, jotta palvelu toimisi. Esimerkki on Windows XP -käyttöjärjestelmästä. Ryhmäkäytäntöjen kautta asetukset määritetään kohdasta *Tietokoneasetukset -> Hallintamallit -> Windowsin osat -> Windows Update* (kuvio 2).



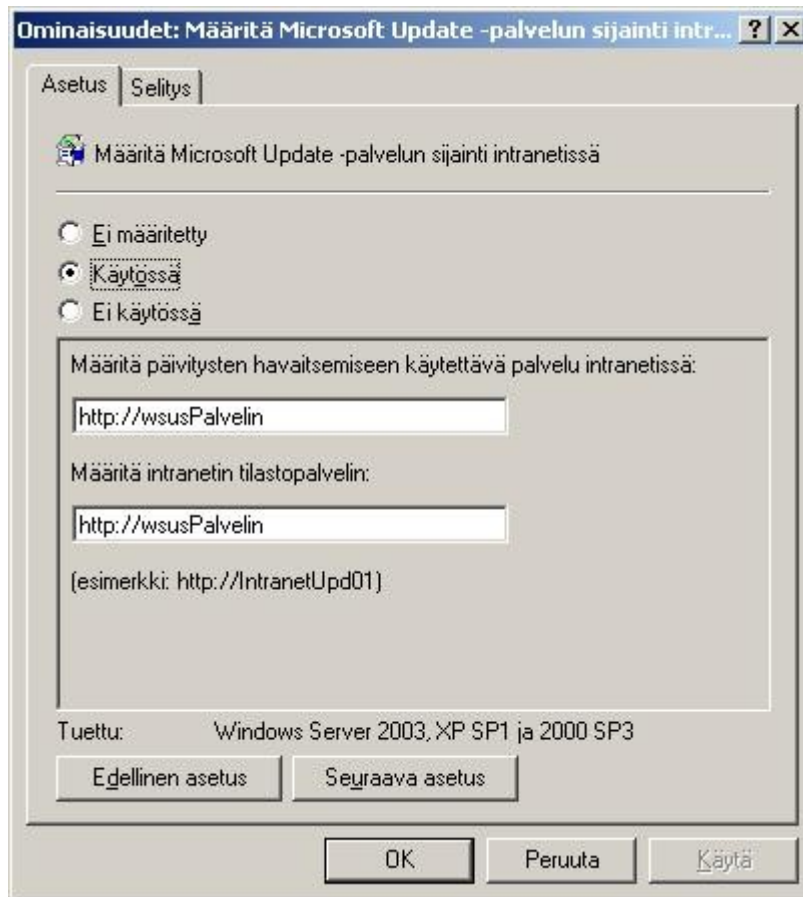
Kuvio 2. Ryhmäkäytäntö-näkymä

Määritä automaattiset päivitykset kohdassa päivitykset latautuvat ja asentuvat automaattisesti valitsemalla vaihtoehdon neljä (4). **Ajoitetun asennuksen suorituspäivä** kohdassa voi valita päivitykset asentumaan joka päivä tai voi valita yhden viikonpäivän jolloin päivitykset asentuvat. **Ajoitetun asennuksen suoritus aika** kohdassa voidaan valita kellonaika jolloin päivitykset lähtevät asentumaan. Vain tasatunnit ovat mahdollisia. Vaihtoehdot ovat väliltä 00-23 (kuvio 3).



Kuvio 3. Ominaisuudet: Määritä automaattiset päivitykset -näky

WSUS-palvelun osoite määritetään kohdassa *Määritä Microsoft Update -palvelun sijainti*. Päivitysten lataamisosoite ja raportointiosoite voivat olla erilaisia, mutta pienessä ympäristössä ne usein ovat samat (kuvio 4).



Kuvio 4. Ominaisuudet: Määritä Microsoft Update -palvelun sijainti -näkyvä

Työasemassa asetukset voidaan määrittää myös Windowsin rekisteristä käsin. Rekisteriarvoja pitää olla vähintään seitsemän kappaletta, jotta päivitykset lataantuvat ja asennetaan automaattisesti WSUS-palvelimelta (kuviot 5).

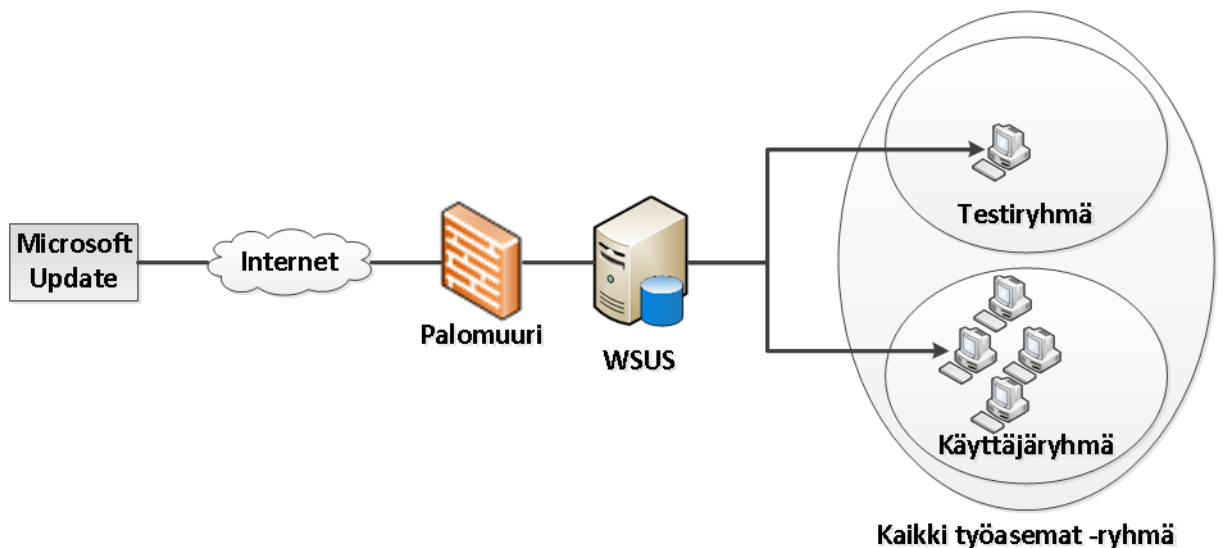
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
"WUServer"=http://wsus_003
"WUStatusServer"=http://wsus_003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000004
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:0000000c
"UseWUServer"=dword:00000001
```

Kuvio 5. WSUS-palvelun käyttöönotto rekisteriarvoilla työasemassa

Helpoin tapa määrittää asetukset asiakaskoneeseen olisi **Active Directory**:n kautta. Tämä tosin edellyttää, että asiakaskoneet olisivat kytketty siihen.

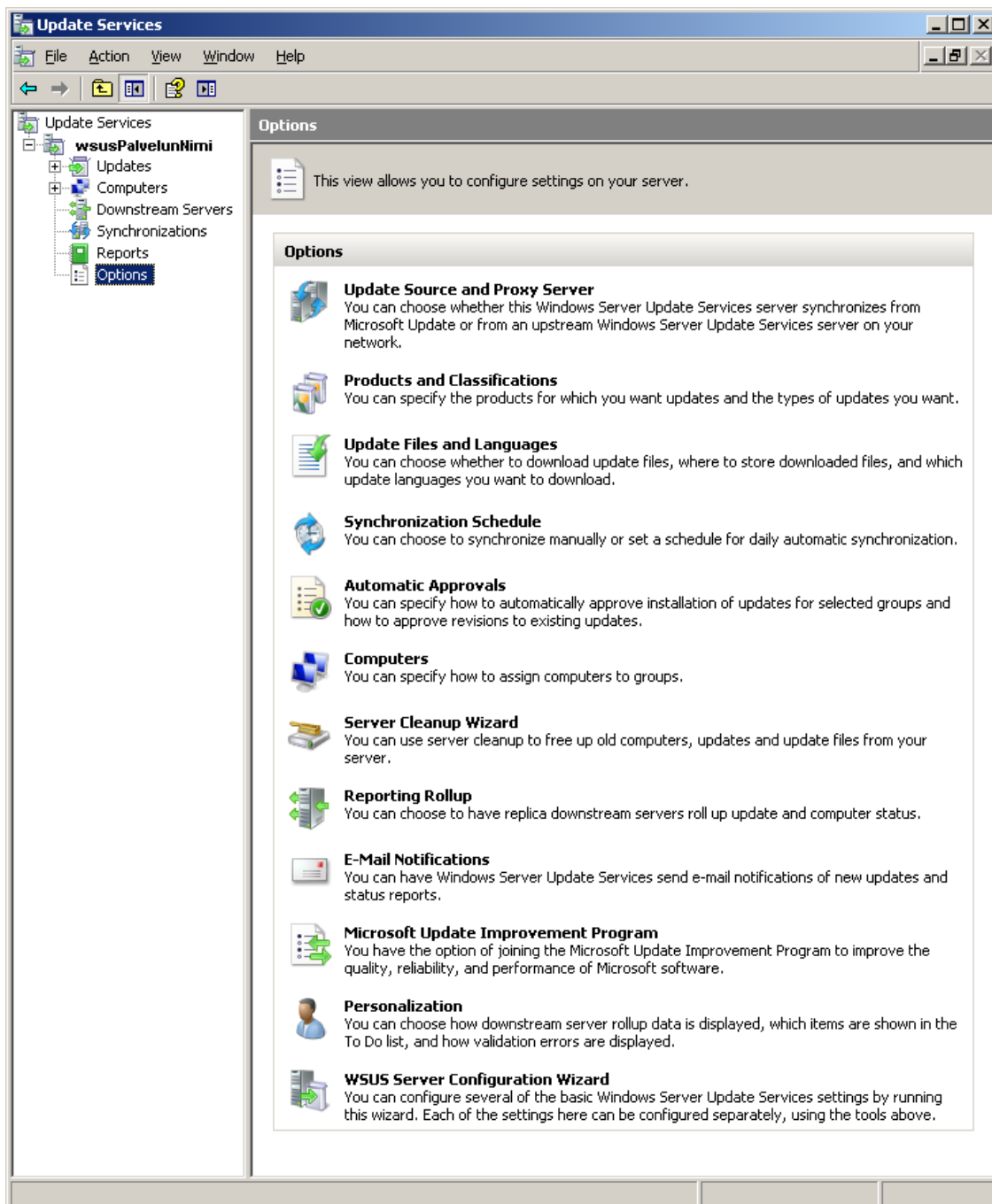
Yksinkertaisen WSUS-palvelun käytön voi toteuttaa kahdella asiakasryhmällä (kuvio 6).



Kuvio 6. WSUS-palvelun yksinkertaistettu käyttö (Microsoft 2010b, 33)

WSUS-palvelussa on syytä olla vähintään kaksi ryhmää, koska päivitysten toimivuudesta kohde järjestelmään ei ole 100 % varmuutta. Näin päivitykset eivät aiheuta ongelmia kaikissa tietokoneissa (kuvio 6).

WSUS-palvelun asennuksen jälkeen palvelimelle pitää siihen tehdä muutama asetus, jotta päivityksiä voisi jakaa asiakaskoneisiin. Asetukset määritellään **Update Services** -konsolista, **Options**-kohdasta (kuvio 7).



Kuvio 7. WSUS-palvelun määrittelyt (Options)

Update Source and Proxy Server -kohtaan määritellään mistä päivitykset ladataan palveluun. Vaihtoehtoja on kaksi, joko Microsoftilta tai toiselta WSUS-palvelulta.

Products and Classifications -kohdasta määritetään Products-välilehdeltä mihin Microsoftin tuotteisiin päivityksiä haetaan. Voidaan valita esim. Office 2003 ja Windows XP. Classifications-välilehdeltä valitaan mihin päivitys luokkaan kuuluvat päivitykset ladataan. Vaihtoehtona esim. **Critical Updates** ja **Service Packs**.

Update Files and Languages -kohdasta määritetään **Update Files** -välilehdeltä ladataanko päivitykset tälle palvelimelle vai lataavatko asiakaskoneet päivitykset **Microsoft Update** -palvelusta. Jos päivitykset halutaan ladata tälle palvelimelle, niin kaikki päivitykset voidaan ladata heti tai vasta sitten kun niitä tarvitaan. Joistain päivityksistä on saatavilla myös ”express” vaihtoehto, jolloin palvelimelle ladataan suuremmat paketit päivityksistä, mutta asiakaskoneille tarvitsee siirtää vähemmän dataa. **Update Languages** -välilehdeltä valitaan kieliversiot päivityksistä. Voidaan valita esimerkiksi **Finnish** ja **English** vaihtoehdot.

Synchronization Schedule -kohdasta voidaan määrittää WSUS-palvelu hakemaan päivitykset joko manuaalisesti tai ajastetusti.

Computers -kohdasta voidaan valita menevätkö WSUS-palvelimeen liitetyt asiakaskoneet **Unassigned Computers** -ryhmään vai ryhmäkäytännöistä määriteltyyn ryhmään.

Nämä määrittäykset riittävät WSUS-palvelun testaamiseen. Seuraava vaihe on luoda asiakaskoneista ryhmiä ja ryhmille määrittää asennettavat päivitykset.

2.4 F-Securen päivittäminen

F-Secure Anti-Virus ja Client Security -ohjelmat voidaan päivittää manuaalisesti tai automaattisesti. Vanhojen 5 ja 6 -versioiden automaattiseen päivittämiseen oli BackWeb-ohjelma. Uudemmat 7, 8 ja 9 -versiot osaavat päivittää itsensä automaattisesti. Tunnis-

tietokantojen päivittäminen onnistuu manuaalisesti käynnistämällä käyttöliittymän tuplaklikkaamalla ”F” kuvaketta Windowsin tehtäväpalkista. Tietokantojen päivitysprosessi käynnistyy klikkaamalla ”Tarkista nyt” (Eng: ”Check Now”) linkkiä.

Työasemissa olevien F-Secure Anti-Virus ja Client Security -ohjelmien tunnistetietokantojen päivittäminen riippuu ohjelmien versioista. Ohjelmien päivittäminen versiosta uudempaan on asia erikseen. F-Securen Anti-Virus ja Client Security -ohjelmiin löytyy manuaalista päivittämistä varten työkaluja. F-Secure fsdbupdate9.exe -työkalulla voi päivittää manuaalisesti version 9 ja versiot 7 ja 8 fsdbupdate.exe -työkalulla. Versioiden 5 ja 6 manuaaliseen virus-tunnistetietokannan päivittämiseen löytyy updateinstaller.exe. F-Securen sivuilta saa virus-tunnistetietokannan ladattua yhtenä tiedostona (latest.zip).

F-Secure Policy Manager on keskitetty hallintatyökalu, josta kaikki siihen liitetyt F-Secure Anti-Virus ja Client Security ohjelmat voivat hakea päivitykset ja asetukset. Asiakasohjelmat myös raportoivat päivitysten läpimenosta sekä kaikesta muusta tietoturvaohjelmistoon liittyvästä.

3 Ohjelmistojen keskitetty päivittäminen Valtion Taidemuseossa

Valtion Taidemuseossa (lyhenne: VTM) Windows XP:llä varustettuja henkilökunnan työasemia on noin 250 kpl ja kannettavia tietokoneita on noin 50 kpl. Kaikki työasemat ja kannettavat tietokoneet on ostettu Valtion taidemuseolle. Leasing-ratkaisustakin on ollut puhetta, mutta siihen ei ole ainakaan toistaiseksi ryhdytty. Tietokoneet jakautuvat neljään eri rakennukseen, joista suurimpina Ateneum ja Kiasma. Koska suurinta osaa tietokoneista käytetään melko kevyesti, on niiden elinkaari pitkä, jopa yli viisi vuotta. Laitekantaa pyritään pitämään yhtenäisenä ja työasemia tilataan mahdollisimman pitkään samanlaisia. Kannettavia tietokoneita on vaikeaa pitää yhtenäisenä, koska niitä tilataan pieniä määriä ja mallit muuttuvat nopeammin kuin pöytäkoneissa.

3.1 Taustaa

Tietokoneiden käyttöjärjestelmiä on aikaisemmin voinut päivittää vain **Novell Client** -hallintaohjelmiston kautta ajettavilla komentosarjoilla (skripteillä) tai suoraan tietokoneelta käsin. Tämä on kuitenkin johtanut siihen, että työasemia ei ole juurikaan päivitetty, koska se on niin työlästä. Novellilla pystyy tekemään raportin, josta näkee Service Pack:in (huoltopäivityksen) version tai sen puutteen, mutta muiden päivitysten puuttuminen on ollut hankala todeta keskitetysti.

Tietokoneita ei ole kytketty Active Directory:iin (aktiivihakemisto), vaan VTm:ssä on käytössä Novell Client. Novell Client:tia käytetään käyttäjien tunnistamiseen ja verkkoon kirjautumiseen. Verkkoon kirjautumisella saadaan käyttöön verkkolevyt (kotihakemisto) ja tulostimet.

Käyttäjien tietokoneosaaminen on hyvin kirjavaa ja harva osaa enempää kuin perustoimisto-ohjelmistojen käytön, jos sitäkään. Tietokoneosaamisen tasosta johtuen käyttäjät ovat melko alttiita roskapostille ja muille verkkohuijauksille. Tietokoneiden saastuminen tulisikin havaita mahdollisimman aikaisin ja ajantasaiset tietoturvapäivitykset tulisi ainakin osan tietokoneiden saastumisesta estää.

Valtion Taidemuseossa palomuuripalvelu on ulkoistettu Nordic LAN & WAN Communication Oy:lle. Palomuri estää hyökkäykset sisäverkon ulkopuolelta, mutta sisäverkossa saastunut tietokone pääsee mellastamaan melko vapaasti. Saastunut tietokone on muutaman kerran päässyt lähettämään roskapostia niin paljon, että Valtion Taidemuseon ip-osoite on joutunut sulkupalveluiden listalle. Tätä ei tosin tapahdu yhtä helposti uudestaan, koska palomuurista ei pääse enää läpi sähköpostiliikenne kuin tietyistä sähköpostipalvelinosoitteista.

Saastuneita tietokoneita voi käyttää muutenkin hyväksi, kuin pelkästään roskapostin lähettämiseen. Tämän takia keskitetty hallinta virusten ja haittaohjelmien havaitsemiseksi on melkein pakollinen. Suurimmassa osassa tietokoneita oli aikaisemmin F-Secure Workstation 5.xx versio, joka suojaa aika puutteellisesti tietokonetta. Virustunnisteti-

tokannan päivitykset ei myöskään tulleet automaattisesti, vaan jouduttiin ajamaan skripti (komentosarja) koneelle kirjautuessa. Koska vuosien saatossa F-Securen virustunnistetietokanta on paisunut yli 65Mt suuruiseksi paketiksi, niin kirjautuminen lähiverkkoon on myös hidastunut.

Uudessa F-Secure Client Security 8.xx versiossa on virusten, vakoiluohjelmien ja rootkit-ohjelmien tunnistuksen lisäksi automaattinen käytönaikainen suojaus. Käytönaikainen suojaus estää matojen ja troijalaisten hyökkäykset, ja siinä on haittakäyttäytymisen seuranta, tietomurtojen esto ja palomuuuri. Automaattisen virustunnistetietokantojen päivityksen ansiosta lähiverkkoon kirjautuminen ei hidastu (F-Secure 2010).

Aikaisemmin käyttöjärjestelmän tietoturvapäivitykset on päivitetty vain uuden tietokoneen asennuksen yhteydessä. Tietokoneiden käyttäjät voisivat itsekin päivittää käyttöjärjestelmään uusimmat päivitykset, mutta sellaista harrastuneisuutta ei löydy juuri muualta kuin tietohallinnosta.

3.2 Lähtötilanne

Valtion Taidemuseossa ei ole ollut käytössä keskitettyä tietoturvaohjelmiston tai käyttöjärjestelmän päivitystä.

F-Secure Policy Manager –palvelu on palvelinpään ohjelmisto. Se on tarkoitettu asiakaskoneiden F-Secure tuotteiden hallintaan. Sillä voi esimerkiksi lähettää asiakaskoneiden tietoturvaohjelmistolle uudet asetukset palomuurille tai ajastaa haittaohjelmien skannauksen. Asiakaskoneiden F-Secure ohjelmistot myös raportoivat kaikesta mahdollisesta Policy Managerille. Ilmoituksia tulee esimerkiksi saastuneista tiedostoista ja verkkohyökkäyksistä. Policy Managerista voi lähettää uudet versiot F-Securen ohjelmistoista asiakaskoneille, jos niitä on saatavilla.

F-Secure Client Security on asiakaspään ohjelmisto joka suojaa työasemaa saastumiselta ja verkkohyökkäyksiltä.

F-Secure Policy Manager –palvelulla voidaan hallita F-Securen tuotteita. Windows-käyttöjärjestelmällisiin tietokoneisiin voidaan lähettää Policy Managerin kautta F-Securen ohjelmistoja, jos ne on kytketty Active Directoryyn. Active Directorystä Policy Manager näkee voidaanko tietokoneeseen luottaa.

Alla on kuvattu ongelmat joita WSUS-palvelun ja F-Securen työkalujen avulla pyrittiin ratkaisemaan.

Ongelmat, joita pyrittiin ratkaisemaan F-Securen uusilla ohjelmistoilla:

- Tietokoneissa ei ole ollut riittävän hyvää/kattavaa ohjelmistoa suojaamaan haittaohjelmilta
- Tietoturvaohjelmiston virustunnistetietokanta ei ole päivittynyt automaattisesti (paitsi ylimääräisen skriptin/komentosarjan avulla)
- Tietoturvaohjelmiston virustunnistetietokantojen päivittäminen on hidastanut verkkoon kirjautumista merkittävästi
- Saastuneesta koneesta ei ole tullut automaattista hälytystä tietohallintoon
- Virustunnistetietokannan vanhentumisesta ei ole tullut ilmoitusta tietohallinnolle, jolloin päivitystarvetta ei ole tunnistettu
- Ei tietoturvaohjelmiston keskitettyä päivitystä (koko ohjelmiston osalta)
- Tietoturvaohjelmiston asetuksia ei ole pystynyt muuttamaan keskitetysti

Ongelmat, joita pyrittiin ratkaisemaan WSUS-palvelulla:

- Tietokoneiden käyttöjärjestelmiin ei ole asennettu uusimpia päivityksiä keskitetysti
- Käyttöjärjestelmien päivitysten keskitetyn seurannan puute.

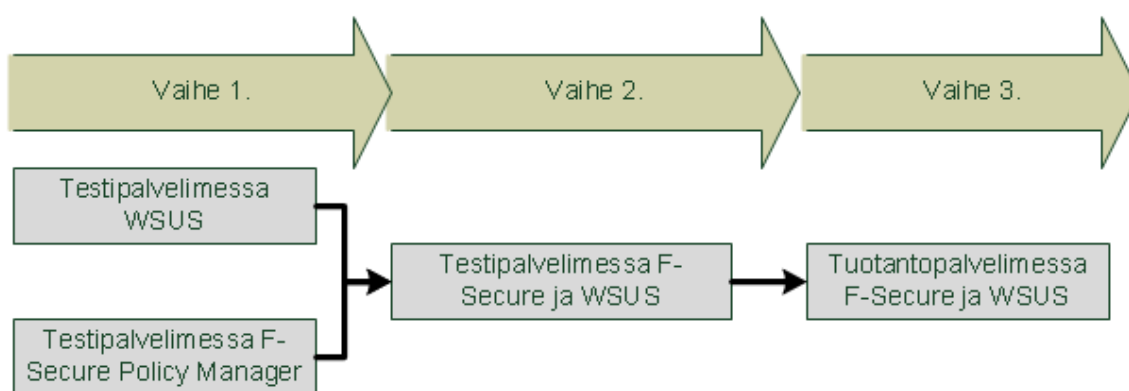
Jatkossa käyttöjärjestelmäpäivitykset hoidetaan WSUS-palvelun (Windows Server Update Services) kautta. WSUS-palvelu on Microsoftin tuotteille suunniteltu palvelinohjelmisto. Sillä voi keskitetysti päivittää melkein kaikki ohjelmistot, joita Microsoft valmistaa. Windows-käyttöjärjestelmät tukevat suoraan WSUS-palvelua, eikä mitään lisäohjelmia Windows-käyttöjärjestelmään tarvita. WSUS-palvelu valittiin käyttöjärjestelmien päivitystyöalukseksi, koska aikaisemmin oli testattu SUS-palvelua (Microsoft Software Update Services) ja siitä oli jo positiivisia kokemuksia. Projektin alussa ei vielä tiedetty

oliko WSUS-palvelu se oikea lopullinen palvelu. WSUS-palvelulla vain päätettiin aloittaa testit ja jos olisi havaittu, että se ei sovellu Valtion Taidemuseon tarpeisiin, niin sitten olisi kokeiltu jotain muuta esimerkiksi Novell ZENworks-palvelua. WSUS-palveluun päädyttiin, koska sen testauksessa ei ilmennyt ongelmia. Myös WSUS-palvelun hinta vaikutti päätökseen, koska se kuuluu palvelinkäyttäjajestelmän lisenssiin, eikä näin ollen aiheuta lisäkuluja.

3.3 Suunnitelma

Suunnitelma oli, että kokeilisin ensin WSUS- ja F-Secure Policy Manager -palveluita erikseen omissa virtuaalipalvelimissa. WSUS-palvelun suhteen olin aika luottavainen, että se saadaan toimimaan lähiverkossa, koska aikaisemmasta SUS-palvelusta (Software Update Services) oli jo jotain kokemusta työkavereillani olemassa. Olin myös ammattikoulun kursseihin liittyen kokeillut ja testaillut tätä uudempaa WSUS-palvelua. Tästä syystä mitään b-suunnitelmaa en lähtenyt edes miettimään. F-Secure Policy Manager -palvelun kanssa tilanne oli vähän eri, koska siitä minulla ei ollut aikaisempaa kokemusta, mutta tiesin, että sitä käytetään myös Haaga-Heliassa. F-Secure Policy Manager -palvelun käyttöohjeesta huomasin, että palvelussa on ainakin yksi toiminto, joka vaatii aktiivihakemistoa. Tämä toiminto on F-Secure tuotteiden jakelu työasemiin. Ennen testaamista en ollut varma estääkö tämä koko F-Securen tuotteiden käytön.

Suunnitelmassa päädyttiin kuvankaltaiseen etenemismalliin.



Kuvio 8. Projektin työvaiheet

3.4 Toteutus

Testasin F-Secure Policy Manager ja Microsoft WSUS -palveluita ensin omissa virtuaalipalvelimissa. Kun palvelut toimivat toivotulla tavalla, niin asensin palvelut samaan virtuaalipalvelimeen. Palveluiden toimiessa hyvin samassa palvelimessa ne asennettiin tuotantopalvelimelle.

3.4.1 Testiympäristö

Kaikki testit päätettiin tehdä virtuaaliympäristössä. Virtuaalisointiympäristöksi valittiin VMware Workstation 6.5 ja sen alustaksi Windows 2003 Server Standard 64bit. Alustan 64-bittisyys on tärkeää, jotta saadaan enemmän muistia käyttöön VMwarea varten (Microsoft 2009a). 32-bittisessä käyttöjärjestelmässä maksimi muistimäärä on 4Gt ja siitä 2Gt voi osoittaa yhdelle prosessille esim. VMwarelle. 64-bittisessä käyttöjärjestelmässä ei tällaisia rajoituksia ole.

Virtuaaliympäristön käyttö on perusteltua, koska siinä on helppoa ja nopeaa monistaa testityöasemia ja -palvelimia.

Osbornen tehotyöasemassa oli aluksi 4 Gt muistia, mutta se tuntui loppuvan jo muutamalla testityöasemalla, joten lisäsin muistia 8 Gigatavuun. Suositeltu minimi muistimäärä virtuaalikoneelle on 128Mt ja suositeltu määrä muistia on 512Mt. Virtuaalikoneilta otin virtuaalimuistin (näennäismuistin) pois käytöstä, koska se vähensi oleellisesti virtuaalikoneiden tarvetta kirjoittaa ja lukea kovalevyltä. Tämä fyysisen kovalevyn jatkuva lukeminen ja kirjoittaminen käytössä näkyi niin, että oli hetkiä jolloin virtuaalikone eikä alustana oleva **Windows 2003 Server** reagoanut näppäimistöön eikä hiireen. Tätä ”jumittamista” saattoi kestää useita minuutteja.

3.4.2 F-Secure Policy Manager

F-Secure Policy Manager 8.0 on mahdollista asentaa sekä Windows että Linux alustalle. Alustaksi valittiin Windows 2003 Server Standard, koska WSUS-palvelu ei toimi Linux

alustalla ja kaikki palvelinten ylläpitäjät osaavat käyttää Windows 2003 Serveriä. Myös Windows 2008 Server olisi käynyt, mutta niitä ei vielä ollut Valtion Taidemuseossa käytössä tämän projektin alkaessa.

F-Secure Policy Manager koostuu kahdesta osasta: palvelinosasta ja konsoliosasta. Konsoliosalla hallitaan palvelinosaa, eikä niiden tarvitse sijaita samalla palvelimella. Tässä projektissa ne haluttiin samalle palvelimelle. Vaikka näistä F-Secure Policy Managerin osista puhutaan erillisinä, niin niitä ei kuitenkaan voi asennusohjelmasta asentaa esim. eri levyosioille. Rekisteristä käsin asennusohjelman voi huijata asentamaan konsoliosan ja palvelinosan eri levyosioille. Tässä olisi se järki, että konsoliosaa ei tarvitsisi varmuuskopioida ja varmuuskopiointinauhaa säästyisi. Suurempi huoli on kuitenkin tulevaisuudessa ilmestyvät päivitykset, joiden asennuksessa voisi tulla ongelmia epästandardin asennuksen johdosta. Konsoliosa vie myös, niin vähän levytilaa, että sillä ei käytännössä ole juuri merkitystä

Manuaalissa mainitut laitevaatimukset tälle palvelulle ovat todella alhaiset, eikä mitään ylimääräisiä ohjelmia tarvita (F-Secure 2009a, 25). Käytännössä väitetyt minimivaatimuksen mukainen 850 Mt (500 Mt palvelin-ohjelmisto + 250 Mt hälytyksiä ja sääntöjä varten + 100 Mt konsoli-ohjelmisto) levytila ei riitä mihinkään, vaan tämä palvelu haukkaa levytilaa melkein 9 Gt. Tähän 9 Gt ei sisälly edes asennuspaketteja tietoturvaohjelmiston jakelua varten työasemille. F-Secure Policy Manager kommunikoi tietokoneiden kanssa Apache web-palvelun kautta.

F-Secure Policy Manager päädyttiin asentamaan eri levyosiolle kuin Windows, jotta Windows ei täytä mahdollisissa virhetilanteissa Policy Managerin levytilaa ja toisinpäin. Muilta osin Policy Manager asennettiin oletusasetuksilla. Oletusportteja ei muutettu, koska muutoin työasemiin asennettaviin F-Securen Internet Security –ohjelman palomuuoreihin olisi tehtävä muutoksia, ennen kuin ne saisivat yhteyden Policy Manager –palveluun.

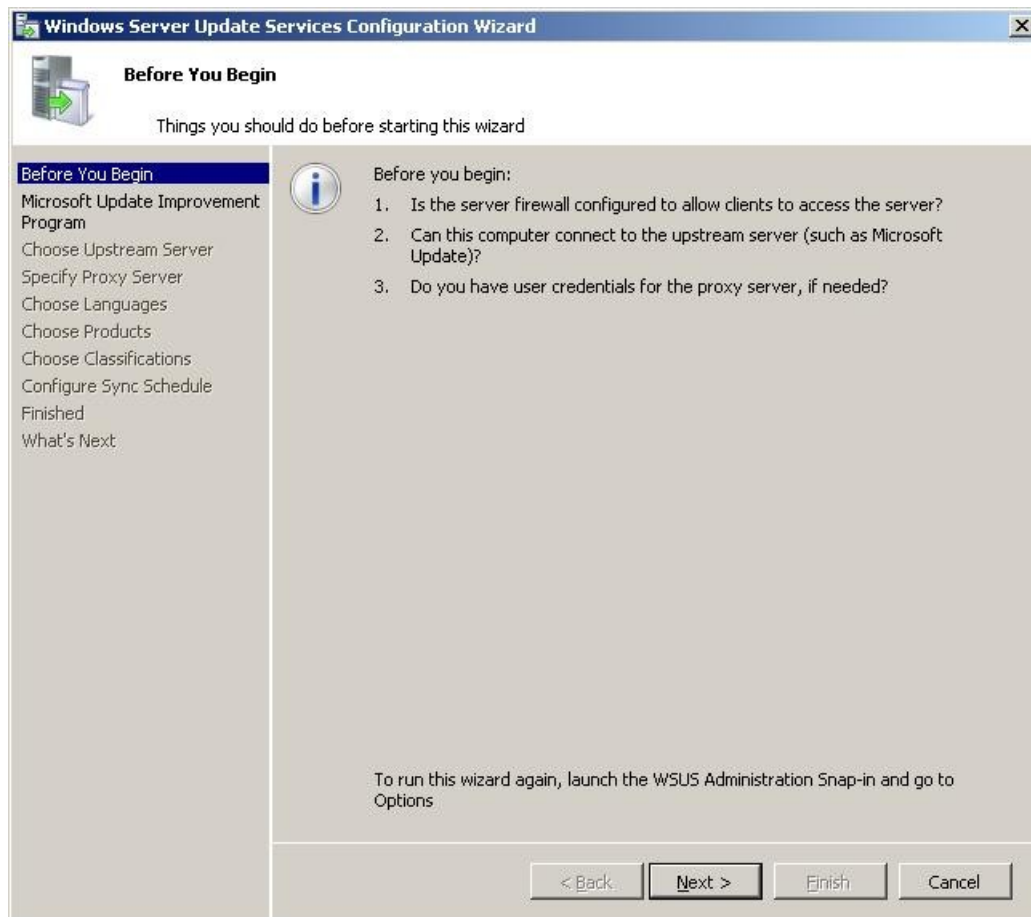
3.4.3 WSUS-palvelu

WSUS-palvelu versio 3.0 SP2 suostuu asentumaan vain Microsoftin palvelinkäyttöjärjestelmien päälle. Laittevaatimukset ovat paljon kovemmat, kuin F-Secure Policy Managerissa ja ne vaikuttavat ehkä jopa realistisimmilta, kuin F-Secure Policy Managerin (Microsoft 2009b, 25). Levytilan minimivaatimus on 20 Gt ja 30 Gt on suositus. Muutama kuukausi WSUS-palvelun käytön aloittamisesta se vie levytilaa melkein 17Gt. WSUS-palvelu asennettiin eri osiolle kuin Windows, enkä testeissä saanut sitä edes toimimaan samalla osiolla kuin Windows tai ainakin ongelmia oli.

WSUS-asennuspaketin lisäksi tarvitaan Internet Information Services (lyhenne: IIS), Microsoft .NET Framework 2.0 tai uudempi, Microsoft Management Console 3.0 ja Microsoft Report Viewer Redistributable 2008. IIS ja Microsoft .NET Framework 2.0 tai uudempi pitää olla asennettuna ennen WSUS-palvelun asennusta, Microsoft Management Console 3.0 ja Microsoft Report Viewer Redistributable 2008 voidaan asentaa myös WSUS-palvelun jälkeen.

WSUS-palvelun yhteysporttiin on kaksi vaihtoehtoa, joko käyttää oletusta porttia 80 tai mukautettua porttia (custom port) 8530. Vaikka custom-vaihtoehdon kenttään pystyykin kirjoittamaan minkä tahansa numeron, niin ainoastaan tuo 8530 portti toimii. Yhteysportiksi valittiin 8530, koska F-Secure Policy Managerissa haluttiin käyttää oletuksia ja siinä on yhteysportti 80 ja samaa porttia ei haluttu käyttää myös WSUS-palvelussa, koska se toisi myöhemmin yhteysongelmia.

Vaikka yleensä asennusvelhot (Setup Wizard) helpottavat asennusta, niin WSUS-palvelun asennuksessa sitä ei kannata käyttää, koska se alkaa heti ladata myös turhia päivityksiä ja niistä eroon pääseminen jälkikäteen on työlästä.



Kuvio 9. WSUS-palvelun asennusvelho (Configuration Wizard)

WSUS-palveluun tulevista päivityksistä valittiin ”express” vaihtoehto, koska se kuormittaa vähemmän sisäverkkoa. Varsinkin yhteys Sinebrychoffin taidemuseoon on melko hidas 10 Mbs ja tällä ”express” vaihtoehdolla sitä kaistaa pystyy säästämään muuhun käyttöön.



Kuvio 10. WSUS-palvelun latausasetuksia palvelimelle

Kuvassa nähdään havainnollisesti ”express” vaihtoehdon tuoma etu, verrattuna ilman ”express” vaihtoehtoa. Käytännössä ”express” versioita ei ole kaikista päivityksistä, vaan niitä on vain muutamista isommista kuten Service Pack:eistä (huoltopäivityksistä).

Express Installation Files Feature

Express installation files enabled



Express installation files disabled



Kuvio 11. Express-asennuspakettien hyödyt/haitat (Microsoft 2010c, 24)

Päivitysten kielistä valittiin suomi ja englanti. Oletuksena on valittu kaikki kielet ja silloin palvelimelle latautuu paljon turhia tiedostoja, mikä täyttäisi levytilaa turhaan.

Microsoft on ryhmitellyt päivitykset yhdeksään ryhmään jotka ovat:

- **Critical Updates** (kriittiset päivitykset)
- **Definition Updates** (päivitykset virus- ja muihin määrittelytiedostoihin)
- **Drivers** (ohjelmia jotka tukevat uusia laitteita)
- **Feature Packs** (Uusia ominaisuuksia, jotka usein lisätään seuraavaan tuotejulkaisuun)
- **Security Updates** (Yleisesti julkaistuja korjauksia tiettyyn tuotteeseen, jotka on kohdistettu tietoturva ongelmiin)
- **Service Packs** (Edellisen tuotejulkaisun jälkeen kertyneet päivitykset, jotka on kerätty yhdeksi isoksi paketiksi. Voi sisältää myös rajallisen määrän asiakkaiden pyytämiä muutoksia tai ominaisuuksia)
- **Tools** (Työkaluja tai toiminto joka auttaa suorittamaan tehtävän tai sarjan tehtäviä)
- **Update Rollups** (Kasautuva joukko päivityksiä, tietoturvapäivityksiä, kriittisiä päivityksiä ja päivityspaketteja koottuna helpompaa jakelua varten)
- **Updates** (Yleisesti julkaistuja korjauksia tiettyyn ongelmaan, joka ei ole kriittinen ongelma tai tietoturvaongelma).

Näistä päätettiin valita **Critical Updates, Security Updates, Service Packs, Update Rollups** ja **Updates**.

WSUS-palvelun kautta päivitettävistä tuotteista valittiin kaikki Office-paketit ja käyttöjärjestelmistä vain Windows XP. Palvelimissa käytetään Windows 2003 Server - käyttöjärjestelmiä ja siihen voisi päivitykset myös ladata WSUS-palvelun kautta, mutta ne on toistaiseksi haluttu asentaa käsin ilman automatisointia. Palvelimia päivittäessä pitää ensin ottaa varmuuskopiot, jotta päivitystä edeltävään tilaan voidaan palata.

3.5 Tulokset

3.5.1 F-Secure Policy Manager

Policy Manageriin työasemat päätettiin järjestellä rakennuksen, kerroksen ja huoneen numeron perusteella. Tällä tavoin saastunut työasema löytyy nopeammin.

Heti käyttöönoton jälkeen alkoi hälytyksiä tulla saastuneista tiedostoista. Jo muutaman viikon jälkeen hälytykset alkoivat vähentyä ja saastuneet koneet saatiin puhdistettua. Ainakin yksi tapaus on tullut tietoon, jossa saastuneeseen koneeseen asennettu **F-Secure Internet Security** –ohjelmisto ei ole löytänyt haittaohjelmaa. Epäilyt haittaohjelmalla saastuneesta työasemasta heräsivät, kun nimipalvelun tapahtumalistauksesta löytyi epämääräisiä osoite kyselyitä. Sieltä löytyi säännöllisiä epäilyttäviä www-osoitteita. Parhaaksi keinoksi havaita tällaiset piiloutuvat (rootkit-tyyppiset) haittaohjelmat todettiin cd-levyltä käynnistettävä haittaohjelmien tunnistusohjelma. Tällaisia cd-levy versioita löytyy esimerkiksi **G Data**:lta ja F-Securelta. Cd-levyltä tietokoneen käynnistämisessä on se etu, että haittaohjelmien on vaikea tai mahdotonta piiloutua tunnistusohjelmalta.

F-Securen Internet Securityn kanssa suurimmaksi ongelmaksi havaittiin virtualisoidut ohjelmat. Ohjelmien virtualisointiin käytämme **Novell ZENworks Application Virtualization** –ohjelmaa. Se otettiin käyttöön vasta F-Secure Policy Managerin jälkeen. Emme löytäneet mitään keinoa, jolla voisi määritellä kansioita tai tiedostoja joita ei tarkistettaisi. Ongelmia aiheuttava komponentti **F-Secure Internet Security** –ohjelmassa on **System Control Server Queries** (DeepGuard 2.0). Virtualisoidut ohjelmat käynnistyvät **System Control** –palvelun kanssa kymenen kertaa hitaammin, kuin ilman. Sitä ei kuitenkaan haluta ottaa pois käytöstä, koska se rampauttaa haittaohjelmien tunnistamista merkittävästi.

3.5.2 WSUS-palvelu

WSUS-palveluun työasemat järjesteltiin vain rakennuksen mukaan, koska jokaiseen järjestelmään ei kannata ylläpidon takia kirjata samaa tietoa. Monissa koneissa ongelmia aiheutti Windows XP:n **Service Pack 3**, joka vaatii levytilaa muita päivityksiä huomattavasti enemmän. Päivitykset eivät osaa katsoa onko levytilaa riittävästi, vaan ne yrittävät asentaa itsensä levytilasta riippumatta.

Toinen ongelmia aiheuttava asia oli päivitysten pakottaminen. Päivitysten pakottamista käytettäessä WSUS-palvelu pakottaa koneen käynnistymään uudestaan, jos joku jonossa olevista päivityksistä sitä vaatii. Näin saadaan päivitykset asennettua nopeammin työasemaan, mutta se häiritsee työaseman käyttöä.

4 Tulosten tarkastelu

Projekti onnistui hyvin ja saavutti sille asetetut tavoitteet. Projektin tavoite oli parantaa Valtion Taidemuseon ohjelmistotietoturvaa ja siinä onnistuttiin hyvin. Onnistumisen voi todeta sillä, että haittaohjelmista saastuneita työasemia alkoi löytyä. Erityisesti työasemista tulevat raportit F-Securesta, joissa ilmoitetaan saastumisesta ilahduttivat. Enää ei tarvitse arvailla mitkä työasemat ovat saastuneet ja milloin, kun siitä on saatavilla ajantasaista informaatiota. WSUS-palvelun käyttöönotto oli vähän ennakoitua hitaampaa ja monimutkaisempaa kuin oli odotettu. Koska testiryhmät ja muut käyttäjäryhmät piti määrittää ennen palvelun käyttöönottoa. Monissa työasemissa oli unohtunut/jäänyt päivittämättä levykuvasta tullut sid-tunnus, josta WSUS-palvelu tunnistaa työaseman.

Tietoturvan osalta on suuri haaste käyttäjien toiminta, koska he eivät ymmärrä tietoturvan merkitystä. Vaikka työasema olisi miten saastunut hyvänsä, mutta jos käyttäjä pystyy jotenkin selviytymään työtehtävistään, niin ei hän siitä mitään kenellekään siitä ilmoita. Käytävällä käyttäjä saattaa ohimennen mainita, että työasema valittaa vähän väliä jotain. Tämän ongelman F-Secure Policy Manager ratkaisee, koska ilmoitukset saastu-

misesta tulee keskitetysti. Esimerkiksi fyysistä tietoturvaa tämä ei ratkaise. Monet käyttäjät eivät lukitse työasemaansa lähtiessään pois työasemalta, vaan jättävät sähköpostit ja muut ohjelmat auki kaikkien ohikulkijoiden ihmeteltäväksi.

4.1 Projektin vaikutukset

Minut palkattiin Valtion Taidemuseolle alun perin tekemään tätä työasemien keskitetyn hallinnan projektia. Olen nyt ollut Valtion Taidemuseolla kaksi vuotta töissä.

Mutta oliko WSUS-palvelusta hyötyä? WSUS-palvelu enemmän lisää työn määrää, kuin vähentää sitä. Aikaisemmin työasemiin ei ole asennettu päivityksiä ja nyt asennetaan, joten työtä tehdään enemmän kuin aikaisemmin. Toisaalta päivitykset kaikkiin työasemiin saadaan asennettua muutaman työaseman päivittämisen vaivalla. Mutta sekoilevatko työasemat vähemmän nyt, kuin ennen työasemien päivittämistä? Tähän on hiukan hankala vastata, koska mitään tilastotietoa ei asiasta meillä ole. Varsinaisen hyödyn mittaaminen tuntuu hiukan hankalalta. Työasemien päivittämättä jättäminen taas tuntuisi vastuuttomalta, koska haittaohjelmat usein käyttävät hyödyksi tunnettuja tietoturva-aukkoja. WSUS-palvelusta saa raportin kaikista siihen liitetystä työasemista, joka helpottaa ylläpitäjien työtä.

F-Secure Policy Manager –palvelusta hyötyvät eniten ylläpitäjät. Nyt ylläpitäjille tulee heti ilmoitus, jos työasemassa on jotain haittaohjelmaan viittaavaa. Myös työasemien sijainnit ovat selvillä, niin tiedetään mistä lähdetään saastunutta työasemaa metsästäämään. Policy Manager –palvelusta saa myös melko hyvän listauksen työasemista, joka auttaa ylläpitäjiä.

Mahdollinen hyöty loppukäyttäjille on se, että heidän työasemansa eivät mene enää niin useasti jumiin haittaohjelmista.

4.2 Projektin haasteita

F-Secure Policy Managerin ja Microsoft WSUS –palveluiden saamisessa samaan palvelimeen oli aluksi yksi hankaluus. Nimittäin Microsoft IIS –palvelu käyttää porttia 80 ja F-Secure Policy Managerin mukana tuleva Apache-palvelu haluaa myös käyttää porttia 80 raportoimiseen. IIS-palvelusta ei pysty suoraan muuttamaan kuunneltavia portteja vaan Windows Server 2003 –käyttöjärjestelmän asennuslevyltä pitää ottaa käyttöön ohjelma jolla kuunneltavia portteja pystyy muuttamaan.

Ennen kuin työasemia kannatti liittää WSUS ja Policy Manager –palveluihin oli tehtävä aika paljon esiselvitystä ja muuta alustavaa työtä. Piti selvittää kuinka monessa työasemassa oli sama yksilöivä sid-tunniste ja kuinka se kannattaa vaihtaa, kuinka paljon työasemat hidastuvat uuden Internet Security –tuotteen takia, mitä eri F-Secure versioita työasemissa on ja kuinka monesta se puuttuu. Työasemat piti myös nimetä yhteneväisellä tavalla ja kirjoittaa Excel-taulukkoon missä ne sijaitsevat. Kaikki tämä alustava työ vei yllättävän paljon aikaa ja ajallisesti se kesti noin kaksi kuukautta. Palvelinohjelmistojen asennukset olivat aika nopeita eikä niihin ei mennyt kuin ehkä viikko ja toinen viikko palveluiden säätämiseen.

4.3 Oma oppiminen

Opin ryhmätyöskentelyä, kun työskentelin tämän projektin parissa kollegoiden kanssa. Olen aikaisemminkin tehnyt opinnäytetyön ammattikoululle, joten en tässä raportin kirjoittamisessa kokenut juurikaan kehittyneeni. Näiden raporttien kirjoittaminen tuntuu edelleenkin tervanjuonnilta ja tämän raportin ehkä vielä vähän pahemmalta. Toivottavasti tulevaisuudessa löytyy raportoinnille joku toinen vaihtoehto, kuin kirjoittaminen.

F-Secure Policy Managerista opin hyvin paljon, koska aikaisemmin en sitä ollut käyttänyt. Palomuuri asetusten muuttaminen ja lähettäminen työasemille vaati ehkä eniten opettelua ja harjoittelua. Policy Managerin käyttöliittymä vaikuttaa melko monipuolisel-

ta, mutta silti siitä tuntui puuttuvan juuri se toiminto jota on hakemassa. Käyttöliittymästä kyllä löytyy perus ja laajennettu versio.

WSUS-palvelusta minulla oli aikaisempaa kokemusta, mutta opin siitä paljon lisää. Työasemien ja päivitysten ryhmittely eri tavoin osoittautui tarpeelliseksi. Kantapään kautta tuli myös huomattua, että päivityksille ei kannata antaa aikarajaa, johon mennessä päivityksen tulee olla asennettuna. Vaikka WSUS-palvelun käyttöliittymä onkin aika yksinkertaisen ja karun näköinen, niin siitä löytyy kuitenkin kaikki tarpeellinen.

4.4 Ideoita ja jatkokehitystä

F-Secure Policy Manager –palvelusta voi myös hallita sallittujen ohjelmien listaa. Tätä voisi hyödyntää niin, että kaikki muut paitsi sallitut ohjelmat olisivat kielletty. Näin pystyisi tietoturvaan parantamaan huomattavasti. Tästä tosin seuraa jatkuva sallittujen ohjelmien listan päivittäminen. Esimerkiksi aina, kun internet-selaimesta tulisi uusi versio, se pitäisi lisätä hyväksytyjen ohjelmien joukkoon. Esimerkiksi kun Firefox 3.6.6 versiosta tulee uudempi versio 3.6.7., niin se pitää lisätä hyväksytyjen ohjelmien listaan, vaikka versio 3.6.6 olisi jo ollut. Tämä ei vie kovinkaan paljoa aikaa, koska ohjelman lisääminen hyväksytyjen ohjelmien listaan vaatii vain ohjelman valitsemisen ohjelmalistasta ja sen lisäämistä hyväksytyjen listaan. Yksittäisen ohjelman lisääminen on aika nopeaa, mutta ohjelmia joista tulee uusia versioita on kuitenkin kymmeniä ja listan päivittäminen alkaa viedä jo aika paljon aikaa. Se kannattako tällaiseen ryhtyä tulisi selvittää ja mahdollisesti testata.

Parannuksena Valtion Taidemuseon yleiseen tietoturvaan voisi ip-osoitteet jakaa toisin kuin dhcp-palvelusta tai sallia tästä palvelusta saaduilla osoitteilla pääsyn vain rajoitettuun verkkoon. Vaihtoehtona voisi olla myös tehdä lista sallittujen laitteiden mac-osoitteista ja nimistä. Tällä hetkellä kaikki laitteet jotka pyytävät ip-osoitetta, saavat sen. Jos ip-osoitteen saisivat vain ne laitteet, joiden nimi ja mac-osoite löytyisivät sallittujen laitteiden listalta, paranisi tietoturva huomattavasti. Vaihtoehtoisesti voisi ottaa dhcp-palvelun kokonaan pois käytöstä ja jakaa osoitteet kiinteästi laitteille. Tällaisen keinon käyttöönottoon löytyy varmasti vaihtoehtoja sitä helpottamaan.

Ylläpitäjiä pitäisi myös kouluttaa tietoturva asioista, että ei tarvitsisi aina mennä yrityksen ja erehdyksen kautta. Vaikka ylläpitäjät huomaavatkin työasemia käyttävien käyttäjien tietoturvasuuteen liittyvät virheet, niin he kuitenkin tekevät itse tietoturvasuuteen liittyviä virheitä. Ei tosin samanlaisia kuin tavalliset käyttäjät, vaan ylläpitotehtäviin liittyviä virheitä, jotka saattavat vaarantaa koko yrityksen tietoturvan. Esimerkiksi jättää puhelimen ilman salasanaa pöydälle, jossa on tekstiviestien joukossa järjestelmävalvojan salasanoja.

Tietoturvaan liittyvistä asioista pitäisi olla prosessikuvaus. Valtion Taidemuseossa työtä tekevien tulisi tietää, että omia tietokoneita ei saa kytkeä lähiverkkoon. Aina hankittaisa uutta laitetta, joka on tarkoitus kytkeä lähiverkkoon, tulisi siitä neuvotella ylläpitäjien kanssa. Tätä ei vielä ole kopiokoneiden hankinnasta päättävät ihmiset sisäistäneet. Vanhoista käyttöjärjestelmistä palvelimissa pitäisi päästä eroon, tai ne pitäisi ainakin eristää muusta verkosta.

Lähteet

About.com 2010. The Unusual History of Microsoft Windows. Luettavissa:
<http://inventors.about.com/od/mstartinventions/a/Windows.htm> . Luettu:
26.11.2010.

Centre of Expertise for Ubiquitous Computing 2009. SUOMALAINEN OHJELMIS-
TOLII-KETOIMINTA 2008 Ohjelmistoyrityskartoitus 2009. Luettavissa:
http://www.swbusiness.fi/uploads/attachments/1252408530_Press_Oskari2009.pdf .
Luettu: 26.11.2010.

Computerworld 2009. Windows 7 steals biggest chunk of share from XP. Luettavissa:
http://www.computerworld.com/s/article/9141606/Windows_7_steals_biggest_chunk_of_share_from_XP . Luettu: 26.11.2010.

F-Secure 2008. F-Secure Policy Manager 8.0 Administrator's Guide. Luettavissa:
http://www.f-secure.com/system/fsgalleries/manuals/fspm800_adminguide_eng.pdf.
Luettu: 16.11.2010.

F-Secure 2010b. Pöytäkoneiden ja kannettavien tietokoneiden suojaus. Luettavissa:
http://www.f-secure.com/fi_FI/products/business/desktops-laptops/client-protection. Luettu: 15.11.2010.

G Data 2010. G Data Malware Report: Half-yearly Report July – December 2010. Luettavissa:
http://www.gdata-software.com/wp-content/uploads/G_Data_MalwareReport_2_2010_EN1.pdf. Luettu: 2.3.2011.

Gartner 2006. Gartner Says Worldwide Antivirus Software Market Increased 13.6 Percent in 2005. Luettavissa:
http://www.gartner.com/press_releases/asset_154006_11.html. Luettu: 26.11.2010.

Gartner 2008. Gartner Says Worldwide Security Software Revenue Reached 20 Per Cent Growth in 2007. Luettavissa:

<http://www.gartner.com/it/page.jsp?id=697307>. Luettu: 26.11.2010.

Gartner 2009. Gartner Says Worldwide Security Software Revenue Grew 18.6 Per Cent in 2008. Luettavissa:

<http://www.gartner.com/it/page.jsp?id=1031712> . Luettu: 26.11.2010.

Jyväskylän yliopisto Tietotekniikan laitos 2011. Ohjelmointi 1 C#. Luettavissa:

<http://kurssit.it.jyu.fi/ITKP102/monistecs/html/moniste.html>. Luettu: 7.4.2011

Microsoft 2003. Windows History - Internet Explorer History. Luettavissa:

<http://www.microsoft.com/windows/WinHistoryIE.aspx> . Luettu: 26.11.2010.

Microsoft 2010. Facts About Microsoft. Luettavissa:

http://www.microsoft.com/presspass/inside_ms.aspx . Luettu: 26.11.2010.

Microsoft 2010a. Memory Support and Windows Operating Systems. Luettavissa:

<http://www.microsoft.com/whdc/system/platform/server/PAE/PAEmem.aspx>.

Luettu: 16.11.2010.

Microsoft 2010b. Microsoft Windows Server Update Services 3.0 SP2 Deployment Guide. Luettavissa:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=113d4d0c-5649-4343-8244-e09e102f9706&displaylang=en>. Luettu: 16.11.2010.

Microsoft 2010c. Deploying Microsoft Windows Server Update Services 3.0 SP1. Luettavissa:

<https://www.microsoft.com/downloads/en/confirmation.aspx?familyid=208e93d1-e1cd-4f38-ad1e-d993e05657c9&displaylang=en>. Luettu: 1.3.2011.

Microsoft 2010d. Windows Server Update Services 3.0 SP2 Operations Guide. Luettavissa:

<https://www.microsoft.com/downloads/en/details.aspx?FamilyID=22395ab7-9234-4eff-b9fd-48f152459aa2&displaylang=en>. Luettu: 2.3.2011.

Mika Hakala, Mika Vainio, Olli Vuorinen. 2006. Tietoturvallisuuden käsikirja. WS Bookwell. Porvoo.

OSNews 2009. The World's First Graphical Browser: Erwise. Luettavissa:

http://www.osnews.com/story/21076/The_World_s_First_Graphical_Browser_Erwise. Luettu: 16.11.2010.

Suomen Internetopas 2010. Luettavissa:

<http://www.internetopas.com/historia>. Luettu: 5.12.2010

The Elder Geek on Windows XP 2010. A Look Back At How We Arrived At Windows XP. Luettavissa:

http://www.theeldergeek.com/windows_timeline.htm. Luettu: 26.11.2010.

Tietojenkäsittelytieteen laitos 2001. Windowsin historia. Luettavissa:

<http://www.cs.helsinki.fi/u/kerola/tkhist/k2001/alustukset/windows/Windowsinhistoria.pdf>. Luettu: 16.11.2010.

Tietokone 2006. Pc-tietokone täyttää 25 vuotta. Luettavissa:

http://www.tietokone.fi/uutiset/2006/pc_tietokone_tayttaa_25_vuotta. Luettu: 26.11.2010.

Tietokone 2010a. Päivän haittaohjelmasaalis: 55 000 kappaletta. Luettavissa:

http://www.tietokone.fi/uutiset/paivan_haittaohjelmasaalis_55_000_kappaletta. Luettu: 26.11.2010.

Tietokone 2010b. Tietoturva petti – uhri joutuu maksamaan 40 miljoonaa. Luettavissa:

http://www.tietokone.fi/uutiset/tietoturva_petti_uhri_joutuu_maksamaan_40_miljoonaa . Luettu: 26.11.2010.

Turku Unix Users Group 1995. Kulttuurihistorian proseminaari. Luettavissa: <http://www.tuug.utu.fi/~jaakko/tutkimus/prose.html> . Luettu: 26.11.2010.

Valtiovarainministeriö 2010. Tietoja valtion tietohallinnosta 2009. Luettavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/04_hallinnon_kehittaminen/20101020Tietoj/Tietoja_tietohallinnosta_2009_netti.pdf. Luettu: 26.11.2010.

Verizon 2009. 285 MILLION RECORDS WERE COMPROMISED IN 2008. Luettavissa: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rpf.pdf . Luettu: 26.11.2010.

Windows Server Update Services Wiki 2010. What Is Windows Server Update Services (WSUS)?. Luettavissa: <http://www.wsuswiki.com/whatiswsus>. Luettu: 1.3.2011.

Xconomy 2009. The Greatest Internet Pioneers You Never Heard Of: The Story of Erwise and Four Finns Who Showed the Way to the Web Browser. Luettavissa: <http://www.xconomy.com/national/2009/03/03/the-greatest-internet-pioneers-you-never-heard-of-the-story-of-erwise-and-four-finns-who-showed-the-way-to-the-web-browser> . Luettu: 26.11.2010.

Liitteet

Liite 1. Projektisuunnitelma

Opinnäytetyön projektisuunnitelma

Eero Teräs

2.3.2011



Sisällys

1	Tausta.....	1
2	Lopputulokset	1
3	Aikataulu ja vaiheet.....	1
4	Työmenetelmät.....	2
5	Henkilöt.....	3

1 Tausta

Opinnäytetyö kuuluu osana ammattikorkeakoulututkintoa. Tässä dokumentissa on kuvattu Eero Teräksen opinnäytetyön projektisuunnitelma.

2 Lopputulokset

Lopputuloksena syntyy opinnäytetyöraportti, Powerpoint-esitys opponointia varten, tiivistelmä, opponoiijien kommentit ja opinnäytetyön ohjaajan kommentit.

3 Aikataulu ja vaiheet

ID	Task Name	Duration	2009												2010												2011		
			tamm	helm	maal	huht	touko	kesä	heinä	elo	syys	loka	marras	joulu	tamm	helm	maal	huht	touko	kesä	heinä	elo	syys	loka	marras	joulu	tamm	helm	maal
1	Ideointi	80d	■																										
2	Määrittely	158d	■																										
3	Menetelmän testaus	151d													■														
4	Toteutus	161d													■														
5	Käyttöönotto	64d																									■		
6	Opponointi	22d																									■		
7	Raportointi	520d	■												■												■		
8	Työn valmistuminen	0d																											

Kuvio 1. Vaiheiden aikataulutus

Ideointi

Ideointi vaiheessa valittiin aihe opinnäytetyölle. Aiheeksi valikoitui Microsoft tuotteiden päivittäminen ja työasemien haittaohjelmien torjunta. Hyväksytetään aihe opinnäytetyön ohjaajalla.

Määrittely

Kartoitetaan nykytila ja suunnitellaan tulevia testejä ja toteutus.

Menetelmän testaus

Menetelmän testausvaiheessa Microsoft WSUS- ja F-Secure Policy Manager –palveluita testataan testiympäristössä. Näin voidaan todeta käytännössä kuinka palvelut toimii ja mitä ne koh-

dejärjestelmältä vaativat. Kun löydetään kohdeympäristöön soveltuva tapa käyttää palveluita, niin yritetään saada ne toimimaan samassa palvelimessa.

Toteutus

Toteutus vaiheessa otetaan käyttöön menetelmän testausvaiheessa toimivaksi havaitut ratkaisut. Palvelut asennetaan ja konfiguroidaan tuotantopalvelimelle.

Käyttöönotto

Käyttöönottovaiheessa pyritään löytämään sopivat menetelmät palveluiden tehokkaaseen käyttöön.

Opponointi

Opponoinnissa esitellään oma työ ja muut opponointiryhmäläiset kommentoivat alustavan raportin, joka on 70 % valmis. Omaa työtä muokataan kommenttien perusteella. Kaksi opponointiryhmäläisten esitystä käydään katsomassa ja töistä annetaan kommentteja.

Raportointi

Raportointi vaihe jatkuu läpi koko projektin ja sen lopputuloksena syntyy raportti työn tuloksesta.

Työn valmistuminen

Työ palautetaan ja se koululla arvioidaan.

4 Työmenetelmät

Työ tehdään Valtion Taidemuseolle heidän tietohallinnon resursseja käyttäen. Myös työympäristö on Valtion Taidemuseo. Työ on edennyt vesiputousmallin mukaisesti, mutta raportointikäytännöt ovat Haaga-Helian opinnäytetyöprosessiohjeistuksen mukaiset. Työn käyttöönotto- vaiheessa on muka erityisesti tietohallinnosta Sampo Vaara.

5 Henkilöt

Taulukko 1. Henkilöt

Rooli	Nimi
Opinnäytetyöntekijä	Eero Teräs
Opponoiija1	Sauli Jurmu
Opponoiija2	Henna Lamminen
Opinnäytetyönohjaaja	Tiina Koskelainen
Kirjallisen esityksen tarkistaja	Kare Ahti
Tekninen konsultti	Sampo Vaara