HAAGA-HELIA
ammattikorkeakoulu

Päivitysten keskitetty paikallisjakelu

Jonne Kurppa

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

2010

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

2010

Tietojenkäsittely

Tekijät Jonne Kurppa	**Ryhmä** TV5Ti
Opinnäytetyön nimi Päivitysten keskitetty paikallisjakelu	**Sivu- ja liitesivumäärä** 52 + 0
Ohjaajat Heikki Hietala	

Microsoft Update -verkkopalvelun kautta voidaan tietokoneille asentaa päivityksiä Microsoftin ohjelmistoille Windows-käyttöjärjestelmistä Office:en. Automaattisten päivitysten avulla tämä voidaan automatisoida ja se on yleensä ottaen riittävän hyvä ratkaisu koneiden päivitystarpeen hoitamiseen varsinkin kotikäytössä.

Yritysmaailman puolella on kuitenkin useitakin syitä olla päästämättä työasemia päivittymään täysin automaattisesti tai edes sallia niille lainkaan pääsyä lähiverkon ulkopuolelle. Vaikka päivitykset voidaan ladata talteen toisella koneella ja asentaa ne sitten käsin verkkorajoitteisille työasemille, se vaatii paljon aikaa ja vaivaa. Parempi ratkaisu onkin ohjata työasemat pyytämään päivityksiä paikalliselta palvelimelta, jossa pyörii Microsoftin päivityssivustoa vastaava palvelu. Päivityksiä voidaan sen avulla hyväksyä asennettavaksi valituille työasemille, kun ne on ensin todettu tarpeellisiksi ja kunnolla testattu.

Tässä raportissa kuvaillaan sopivan päivitystenjakelujärjestelmän valinta, testaus ja käyttöönotto kohteena toimineelle yritykselle.

Windows Server Update Services (WSUS) valittiin testaukseen, sillä se täytti kaikki sille asetetut vaatimukset ollen samalla myös vapaasti asennettavissa kaikille Windows 200x -pohjaisille palvelimille. Testiin valituille työasemille ajettiin useaan kertaan kaikki asennettavissa olevat päivitykset aina välissä palauttaen ne testin alussa vallinneeseen tilaansa levykuvien avulla.

Päivitykset asentuivat enimmäkseen ongelmitta, tosin joidenkin päivitysten asennusjärjestystä voisi Microsoft hiukan miettiä uudelleen.

Testauksen jälkeen WSUS hyväksyttiin laajempaan käyttöön ja yrityksen työasemat ohjattiin käyttämään sitä päivityslähteenään. Lopuksi WSUS-palvelin siirrettiin pääkonttorin palvelintiloihin.

Asiasanat
WSUS, tietoturva, päivittäminen, Windows, atk-tuki, lähiverkko.

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

2010

Tietojenkäsittely

Authors Jonne Kurppa	**Group** TV5Ti
The title of thesis Centralized Local Distribution of Updates	**Number of pages and appendices** 52 + 0
Supervisors Heikki Hietala	

Microsoft Update is a web-based service that allows computers to get updates for Microsoft's various products like most versions of the Windows Operating System and Office. With Automatic Updates this can be done automatically and it is mostly a good enough solution to get all the necessary updates for Microsoft's software especially for home users.

However, in corporate networks there are many reasons for not letting workstations to update themselves automatically or even access the web at all. While the updates can be downloaded from a separate computer and then be manually installed to these restricted workstations, the process is time consuming and hence a better solution is to direct the workstations to request the updates from a local server that is configured to act like a Microsoft's own update site on the web. Updates can then be approved for installation on selected workstations after they are reviewed to be necessary and properly tested.

This document describes the process of determining a suitable solution for distributing updates locally, testing it and finally deploying it for a target company.

Windows Server Update Services (WSUS) was chosen for testing because it delivered all the key requirements while being free to use in any server running a Windows Server 200x based operating system. Updates were ran on selected workstations multiple times by restoring them to unupdated state from disk images made at the beginning of the tests.

Updates installed mostly without problems, although for some updates Microsoft could think again about the order they are offered to be installed.

After the tests WSUS was cleared for full deployment and workstations were directed to use it as their update server. Finally the server was transferred to headquarters's server room.

Key words
WSUS, Information Security, Updating, Windows, IT-support, Local Area Network.

Sisällys

1 Johdanto....1
1.1 Projektin tavoite ja rajaukset....1
1.2 Käsitteet....2
2 Viitekehys....3
2.1 Käyttöjärjestelmä ja ohjelmat....3
2.2 Päivittäminen....4
2.2.1 Patch Tuesday....4
2.3 Työasemakohtaisesti ajettavat päivittämisvaihtoehdot....5
2.3.1 Windows Update....5
2.3.2 Automatic Updates....6
2.3.3 Office Update....7
2.3.4 Microsoft Update (MU)....7
2.3.5 Windows Update Catalog (WUC)....8
2.3.6 Microsoft Update Catalog (MUC)....13
2.4 Palvelimelta käsin hallitut päivitysten jakeluratkaisut....17
2.4.1 Software Update Services (SUS)....17
2.4.2 Windows Server Update Services (WSUS)....18
2.4.3 Systems Management Server (SMS)....19
2.5 Apuohjelmistot....21
2.5.1 Microsoft Baseline Security Analyser (MBSA)....21
2.5.2 Active Directory (AD)....21
3 Empiirinen osuus....22
3.1 Lähtötilanne....22
3.2 Esivalmistelut....24
3.3 Tarpeiden ja resurssien kartoitus....26
3.3.1 Käytettävissä olevat resurssit....27
3.4 Muokattu toteutussuunnitelma....28

3.4.1 Viitemateriaaliin tutustuminen....28
3.4.2 Testiympäristön pystytys, laitteiden verkotus ja hallinta....28
3.4.3 Palvelimen pystytys ja ohjelmistojen asennus....28
3.4.4 Testikoneiden liittäminen palvelimen alaisuuteen....29
3.4.5 Päivitysten valinta ja hallinta....29
3.4.6 Testaus, toistot....29
3.4.7 Käyttöönotto....30
3.4.8 Seuranta ja raportointi....30
3.5 Suunnitelman toteutus käytännössä....31
3.5.1 Toteutusvaihtoehdon valinta....31
3.5.2 Testiympäristö....31
3.5.3 WSUS-palvelimen tarvitsemien palvelujen ja ohjelmien asennus....32
3.5.4 WSUS-palvelimen asennus ja asetusten määrittely....32
3.5.5 Työasemien ohjaus WSUS-palvelimelle....34
3.5.6 WSUS-palvelun hallintakonsoli....39
3.6 Testaus ja käyttöönotto....44
3.7 Seuranta ja tulokset....46
4 Yhteenveto....48
Lähteet....50

1 Johdanto

Windows-työaseman asettaminen päivittämään itsensä automaattisesti Windows Update -palvelun kautta riittää sinällään melko hyvin pitämään minimissään työasemien tietoturvariskit Microsoftin ohjelmistojen osalta. Tämä sillä oletuksella, että virustorjunnasta, palomuurista ja tiukasta käyttöoikeuksien rajoittamista on pidetty huolta. Automaattisissa päivityksissä on kuitenkin omat ongelmansa, esim. yrityksen intranetissä voi olla kytkettynä koneita, joiden pääsy verkon ulkopuolelle on syystä tai toisesta estetty ja niinpä ne voivat ylläpidon resurssipulassa jäädä päivittämättä pitkiksikin ajoiksi kunnes jokin syy pakottaa tukihenkilön käymään paikalla.

Tällaisista koneista muodostuu ajan myötä suuri riski, joka voi realisoitua, kun vanhakin haittaohjelma pääsee jotain tietä yritysverkon sisälle ja tartuttaa päivittämättä jääneet työasemat. Vaikka sisäverkkoon rajatuille koneille pystyttäisiinkin ehtimään ajaa päivitykset vaikkapa avaamalla niille yksi kerrallaan yhteys ulos, ei kaikkien päivitysten asentaminen jokaiselle työasemalle aivan heti niiden ilmestyttyä ole sekään välttämättä aivan viisasta. Jotkin päivitykset voivat muuttaa ohjelmistojen toimintaa ja siten samalla rikkoa yrityksen jonkin sisäisen järjestelmän, kuten vaikkapa selainpohjaisen käyttöliittymän.

On myös huomattava, ettei jokaisen koneen käyminen lataamassa erikseen päivityksensä Microsoftin palvelimelta ole kaikkein tehokkainta kaistankäyttöä ja että esim. tärkeitä esityksiä pitävillä koneilla ei päivitysten ajon jälkeen mahdollisesti tulevaa uudelleenkäynnistyspyyntöä välttämättä haluta nähdä yllättäen. Tämä opinnäytetyö pureutuukin Windows-pohjaisen lähiverkon koneiden tietoturvapäivitysten jakelun keskittämisen suunnitteluun, testaukseen ja toteutukseen. Työ on toteutettu yrityksessä, jossa koneiden määrän kasvaessa oltiin todettu olevan aika ottaa käyttöön omassa hallinnassa oleva päivitysten jakelujärjestelmä.

1.1 Projektin tavoite ja rajaukset

Tavoitteena olisi pystyä jakamaan Windows/Microsoft Update -sivuston tarjoamat päivitykset kohdeyrityksen koneisiin yrityksen omalta palvelimelta. Lisäksi päivitysten jakelu tulisi olla porrastettavissa useampaan ryhmään koneiden kriittisyyden ja tarpeiden mukaan, jottei esim. tuotanto häiriinny päivityksen muuttaessa tapaa jolla tulostuspohjien makrot toimivat. Opinnäytetyössä käsitellään Microsoftin ohjelmistoja käyttävän yrityksen tarpeita vastaavan päivitystenjakelujärjestelmän valintaa, testausta ja käyttöönottoa.

1.2 Käsitteet

Koska käsiteltävä aihe sisältää paljon vieraskielisiä termejä, luetellaan tässä joitakin niistä selitteiden kera. Tekstissä joidenkin monisanaisten palvelujen ja ohjelmien nimet ovat useamman kerran toistuessaan saatettu korvata lyhenteillä. Palvelinkäyttöjärjestelmien ollessa yleensä vain englanninkielisiä, ei niiden joillekin toiminnoille edes välttämättä ole yleisti hyväksyttyjä käännöksiä.

- Järjestelmä (system) sisältää tietokoneen ja sen ohjelmistot.
- Järjestelmänvalvoja on henkilö, jonka käyttäjätilille on myönnetty ylläpito-oikeudet.
- Pääkäyttäjä pystyy tekemään hallintatoimenpiteitä omalla koneellaan.
- Käyttäjä on kuka tahansa tietokoneelle kirjautunut henkilö.
- Toimialue (Domain) on palvelinten sekä käyttäjä- että tietokonetilien yhteenliittymä.
- Käyttäjätili sisältää käyttäjän tiedot.
- Tietokonetili sisältää tietokoneen tiedot.
- Rekisteri (registry) on Windowsin asetusten tietokanta
- Ohjattu toiminto (wizard) eli velho hoitaa asetusten määrityksen vaiheittain, jotta mitään tarpeellista asiaa ei vahingossa jäisi tekemättä.
- Skripti (script) tarkoittaa joukkoa komentoja, jotka suoritetaan komentotulkin avulla.
- Komentorivikomento on komentorivissä suoritettava komento.
- Korjauspaketti (Service Pack) on kokoelma kaikista aiemmista päivityksistä ja voi lisätä myös uusia ominaisuuksia. Lyhenne ilmaistaan korjauspaketin numeron kera.
- Palvelin (server) on tietokone, joka tarjoaa erilaisia palveluita verkon muille laitteille.
- Työasema on tietokone, joka toimii käyttäjien työvälineenä.

2 Viitekehys

Tässä osiossa käydään läpi erinäisiä päivitysten jakelu- ja asennusvaihtoehtoja. Aluksi kuitenkin tarkastellaan mikä on käyttöjärjestelmän tehtävä ja miksi sille ja sen päällä ajettaville ohjelmistoille tulisi asentaa päivityksiä.

2.1 Käyttöjärjestelmä ja ohjelmat

Ennen käyttöjärjestelmiä yksinkertaisimpienkin tehtävien suorittaminen tietokoneella vaati käyttäjää syöttämään laitteelle konekielellä ohjeet esim. siitä mitä lukuja haluttiin summata ja miten saatu arvo tulostettaisiin näkyville. Suoritettavien ohjelmien piti siis sisältää oman tehtävänsä lisäksi myös ohjeet kaikkien tarvittavien oheislaitteiden käytölle, jotta esim. näyttö, hiiri ja tulostin olisivat käytettävissä. Lisäksi ohjelmista olisi pitänyt tehdä uudet versiot jokaista erilaista laitekokoonpanoa varten. Eikä pidä unohtaa massamuistien olleen muinoin todella pieniä ja kalliita, joten oheislaitteiden ohjauskoodin sisällyttäminen jokaiseen ohjelmaan ei ollut halpaa lystiä vaikka koodaajat olisivat työskennelleet ilmaiseksi.

Ratkaisuksi ongelmaan tarvittiin erityinen ohjelma, jonka päällä muut ohjelmat ajettaisiin ja se toimisi rajapintana niiden ja tietokoneen oheislaitteiden välillä. Tämä ohjelma, eli käyttöjärjestelmä on siis ”perussäännöstö, jonka mukaan keskussuoritin lukee tietoa ja ohjelmia, käsittelee tietoa ja tulostaa sitä”. (Kytöhonka 1989, 900.)

Käyttöjärjestelmää on myös kuvattu orkesterinjohtajaksi, joka ohjaa tietokoneen eri osien toimintaa ja mahdollistaa saman ohjelman suorittamisen erimerkkisissäkin tietokoneissa, mikäli niissä on sama käyttöjärjestelmä. (Kaiken maailman keksinnöt 1994 1993. 259.)

Käyttöjärjestelmien ansiosta ohjelmistojen kehittäjien ei enää tarvinnut jokaisen osata koodata tukea kaikille markkinoilla oleville laitteille, koska niille tarvittavat ajurit jäivät laitevalmistajien koodattaviksi. Tosin vielä pitkän aikaa levynkäyttöjärjestelmien, kuten Microsoft DOS, valtakaudella oli jokaisen pelin vielä tuettava suoraan useita peli- ja näytönohjaimia sekä varsinkin äänikortteja. ”Windows 95:n myötä äänikorttikohtainen koodaus siirtyy historiaan: korttivalmistajat kehittävät 95-ajurit, ohjelmoijat koodaavat soittorutiinit ja muusikot säveltävät.” (Mäntylahti 1996, 14.)

2.2 Päivittäminen

Käyttöjärjestelmien ja ohjelmistojen päivittämiselle voidaan löytää kolme tarvetta: virheiden korjaus, uudet ominaisuudet sekä haavoittuvuuksien paikkaaminen. Vaikka haavoittuvuudet voidaankin lukea virheiksi, eivät ne välttämättä ilmene normaalissa käytössä eivätkä siten haittaa suoraan ohjelman käyttöä.

Virheiden poisto ja uudet ominaisuudet ovat jo itsessään hyviä syitä päivittämiseen, mutta todellinen tarve pitää kaikki ohjelmistot jatkuvasti ajan tasalla on kuitenkin tietoturvan ylläpito. Internetistä voidaan haavoittuvalle koneelle päästä livahtamaan haittaohjelmia, jotka esim. tekevät siitä roskapostin levittäjän tai mahdollistavat koneen etäkäytön. (Keränen 2005, 63.)

Aukot tietoturvassa uhkaavat jo pelkästään mitä tahansa verkkoon liitettyä kotikonettakin. Yritysten lähiverkossa olisi saatavilla huomattavasti arvokkaampaa dataa, joten niihin myös voidaan tehdä varta vasten räätälöityjä hyökkäyksiä. Ohjelmallisten päivitysten lisäksi olisi myös syytä muistaa ylläpitää henkilökunnan tietoturvaohjeistusta, etteivät esim. parkkipaikalta löytyneitä USB-tikkuja tungettaisi yrityksen työasemiin. (Stasiukonis 2006.)

2.2.1 Patch Tuesday

Mikrosoftin nykyistä päivitysten julkaisukäytäntöä on alettu kutsua päivitystiistaiksi, koska uudet päivitykset julkaistaan joka kuun toisena tiistaina. (Microsoft TechNet 2010.)

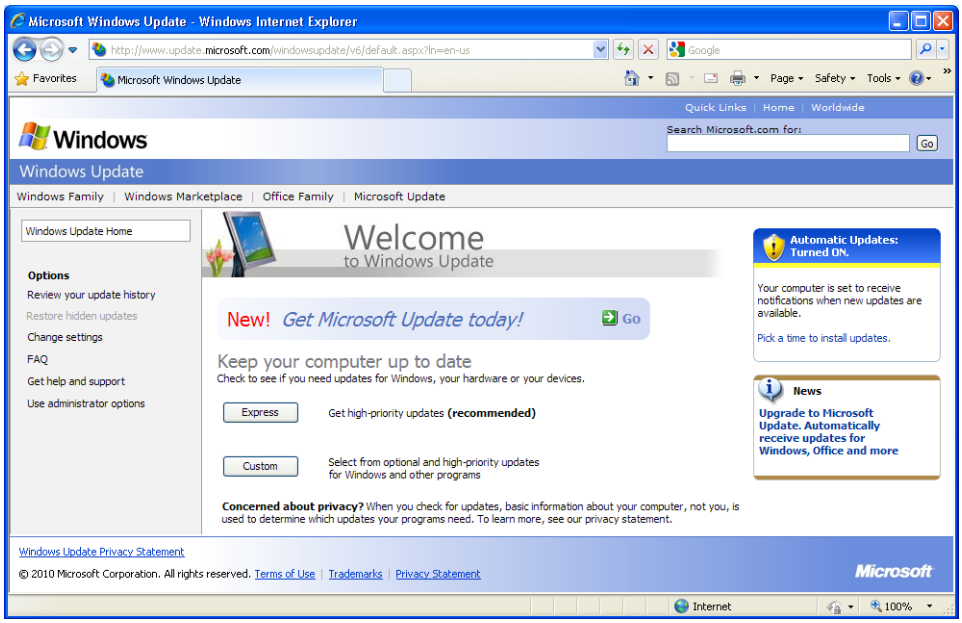
Päivitystiistain hyvänä puolena voitaneen nähdä sen antavan ylläpidolle joka kuukaudelle tarkan päivämäärän jolloin tulisi osata odottaa päivityksiä ja niiden asennuksen jälkeen voi hengähtää helpotuksesta kunnes jokin muu ongelma ilmenee.

Käytäntöä on myös kritisoitu mm. siksi, että monet haavoittuvuudet saavat odottaa paikkausta seuraavaan päivitystiistaihin ja korjaus saattaa myöhästyä siitäkin. Lisäksi päivitysten julkaisun ennustettavuus yhdistettynä niiden asennuksen viivästymiseen yrityksissä esim. kattavan testauksen takia mahdollistaa myös haittaohjelmien kehittäjät keskittämään hyökkäyksensä heti päivitysten julkaisun jälkeen käyttäen hyväksi juuri julkituotuja aukkoja. (SearchSecurity 2007.)

2.3 Työasemakohtaisesti ajettavat päivittämisvaihtoehdot

Vaikka osa työasemien itsensä kautta toteutettavista päivitysmenetelmistä voidaan määrittää ajamaan päivitykset automaattisesti, niitä yhdistää se seikka, että jokainen työasema joko hakee erikseen päivityksensä netistä tai ylläpidon on koottava haluamansa päivitykset esim. CD:lle ja asennettava ne siitä jokaiselle työasemalle erikseen. Automaattinen asennus ajaa koneille kaikki päivitykset, käsin valinta konekohtaisesti vaatii aikaa ja kärsivällisyyttä, eikä koostelevyn teettäminen ja sen kanssa koneiden päivittäminen vähennä muuta kuin ulkoapäin ladattavan datan kokonaismäärää. Lisäksi koostelevyyn on tietenkin haettava kaikki mahdollisesti hyödylliset päivitykset, jonka jälkeen ongelmana onkin asentaa niistä konekohtaisesti vain tarpeelliset päivitykset.

2.3.1 Windows Update



Kuva 1: Windows Update -palvelun pääsivu.

Windows Update on Windows 98:n julkaisun yhteydessä avattu palvelu, jonka avulla siihen yhteyttä ottava työasema saa listan sille tarjolla olevista päivityksistä, jotka käyttäjä voi valita asennettaviksi. Windows Update kommunikoi työaseman Windows-pohjaisen käyttöjärjestelmän kanssa ActiveX-komponentin kautta, mistä johtuen se vaatii käytännössä käyttämään Microsoftin Internet Explorer -selainta. (McFedries 1999, 322; Ohio Land Title Association 2007.)

Alunperin käyttäjien piti itse muistaa käydä sivustolla säännöllisesti, mutta pian Microsoft tarjosi Windows Update -palvelun kautta ladattavaksi kriittisten päivitysten ilmoitustoimintoa, joka nimensä mukaisesti antoi ruudulle ilmoituksen, kun uusia päivityksiä oli saatavilla.

Windows Update jakaa päivitykset kolmeen luokkaan:

- High priority/Ensisijainen: Kriittiset päivitykset, jotka tulisi yleensä asentaa kaikkiin työasemiin.
- Software (optional)/Ohjelmistot, valinnaiset: Uusia ominaisuuksia tai kokonaan uusia ohjelmia.
- Hardware (optional)/Laitteisto, valinnaiset: Laiteohjainpäivityksiä, yleensä vanhentuneita.

(Kivimäki 2005b, 133.)

Päivitysten lataaminen ja asentaminen Windows Update -palvelun kautta vähänkään laajemman konekannan kanssa ei ole kovinkaan tehokasta, sillä päivitykset pitää ladata jokaiseen koneeseen erikseen Microsoftin palvelimelta, mikä mm. kuormittaa verkkoa. Päivitettävät koneet tarvitsevat pääsyn lähiverkon ulkopuolelle ja ylläpidon on joko ehdittävä hoitaa kaikkien koneiden päivittäminen itse tai annettava muulle henkilökunnalle riittävät oikeudet päivitysten ajamiseen. Windows Update jäänee nykyään pitkälti uunituoreen työaseman päivittämiseen ajan tasalle ennen sen viemistä kentälle. Silloinkin Windows 2000 ja uudemmat versiot kannattaisi päivittää uudemman Microsoft Update -sivuston kautta.

2.3.2 Automatic Updates

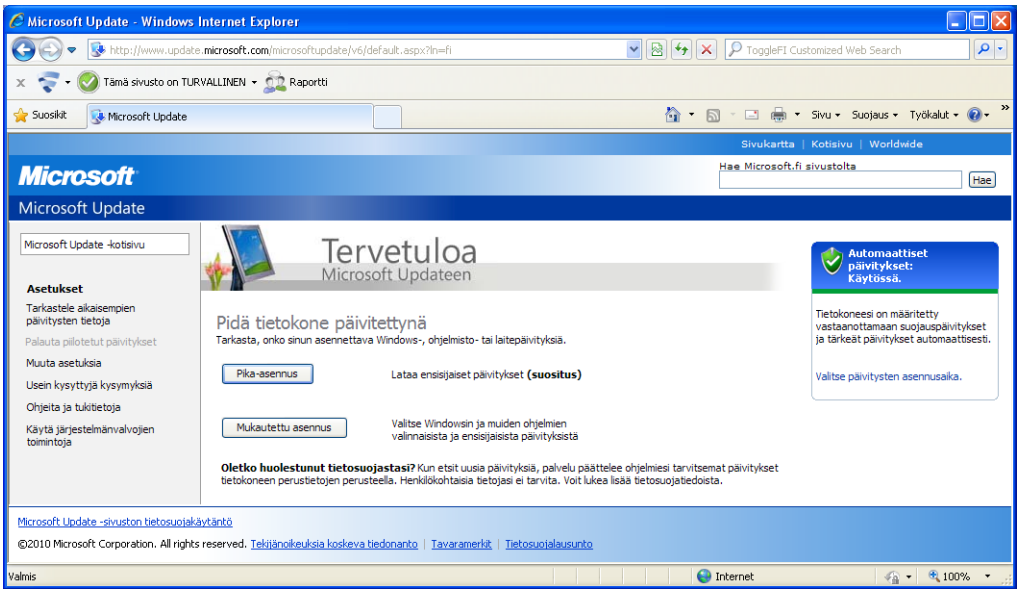
Windows ME:n julkaisun myötä tuli mahdolliseksi automatisoida päivitysten lataaminen, minkä lisäksi ne voitiin myös määrittää asentumaan automaattisesti tai ainakin huomauttaa uusien päivityksien olevan saatavilla. Microsoft ei kuitenkaan tarjoa automaattisten päivitysten kautta koneille valinnaisia päivityksiä, vaan ne pitää yhä hakea joko WU, MU, MUC tai Microsoft Download Center -sivustojen kautta. Mikäli päivitysten asentaminen jätetään työaseman haltijan vastuulle, tulee hänellä myös olla pääkäyttäjän oikeudet kyseiselle koneelle tai päivitykset jäävät odottamaan kunnes ylläpito kirjautuu sisään ja ajaa ne. Automaattinen asennus taas ei anna alemmilla oikeuksilla konetta käyttäville mitään mahdollisuutta viivästyttää uudelleenkäynnistystä. Olisi myös suositeltavaa ettei päivityksiä ajettaisi koneille testaamatta ensin hallitussa ympäristössä etteivät ne riko muiden ohjelmien toiminnallisuutta. (Kivimäki 2005b, 249.)

Palvelimelta käsin hallittavat päivitysjärjestelmät käyttävät yleensä automaattisten päivitysten toimintoa ohjaten vain työaseman hakemaan automaattiset päivityksensä eri osoitteesta ja sallivat esim. uudelleenkäynnistyksen viivästämisen ilman järjestelmänvalvojan oikeuksiakin. Tätä kautta automaattisten päivitysten joukkoon voidaan myös lisätä valinnaisia ohjelmistopäivityksiä.

2.3.3 Office Update

Windows Update -sivuston tarjotessa päivityksiä vain Windowsin mukana tuleviin ohjelmistoihin, sen rinnalle luotiin oma sivustonsa Microsoft Office -tuoteperheen päivityksille. Sivusto suljettiin vuonna 2009 Microsoftin liittäessä sen palvelut Microsoft Update -sivuston yhteyteen. Samoihin aikoihin Microsoft Office 2000 siirtyi pois jatketun tuen piiristä eikä Microsoft Update tarjoa sille lainkaan päivityksiä vaan ne on osattava etsiä omin neuvoin Microsoftin muilta sivustoilta. (Office Sustained Engineering, 2009.)

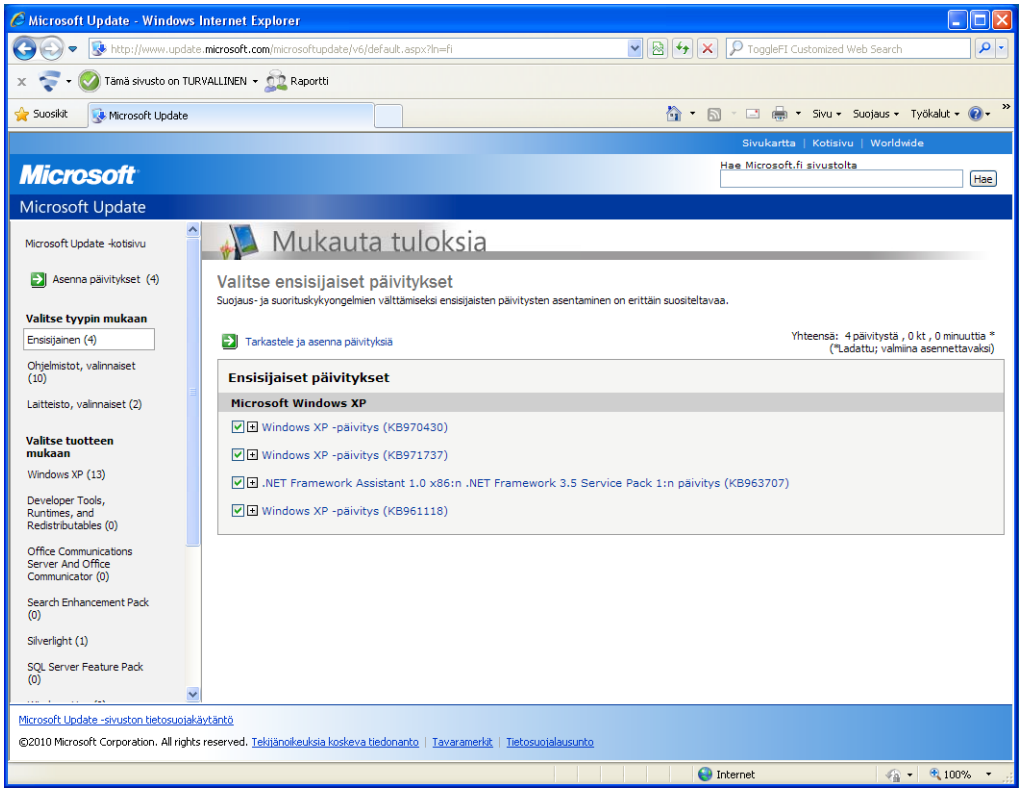
2.3.4 Microsoft Update (MU)



Kuva 2: Microsoft Update -palvelun pääsivu.

Microsoft Update on Windows Update ja Office Update -sivustot korvaava palvelu, jonka kautta tarjotaan laajempaa päivitysvalikoimaa. Oleellisimpana erona Windows Update -palveluun nähden Microsoft Update ei tarjoa päivityksiä Windows 2000 käyttöjärjestelmää ja Office XP toimisto-ohjelmistoa vanhemmille tuotteille. Palvelu julkistettiin vuonna 2005 (HelpWith-

Windows.com, 2005). Käyttöliittymältään Microsoft Update on lähes identtinen Windows Update -sivuston kanssa, palveluiden pääsivuilta voi havaita pieniä eroavaisuuksia, mutta käytännössä molemmissa on sama rakenne ja päivitysten haku tehdään samasta napista painamalla.



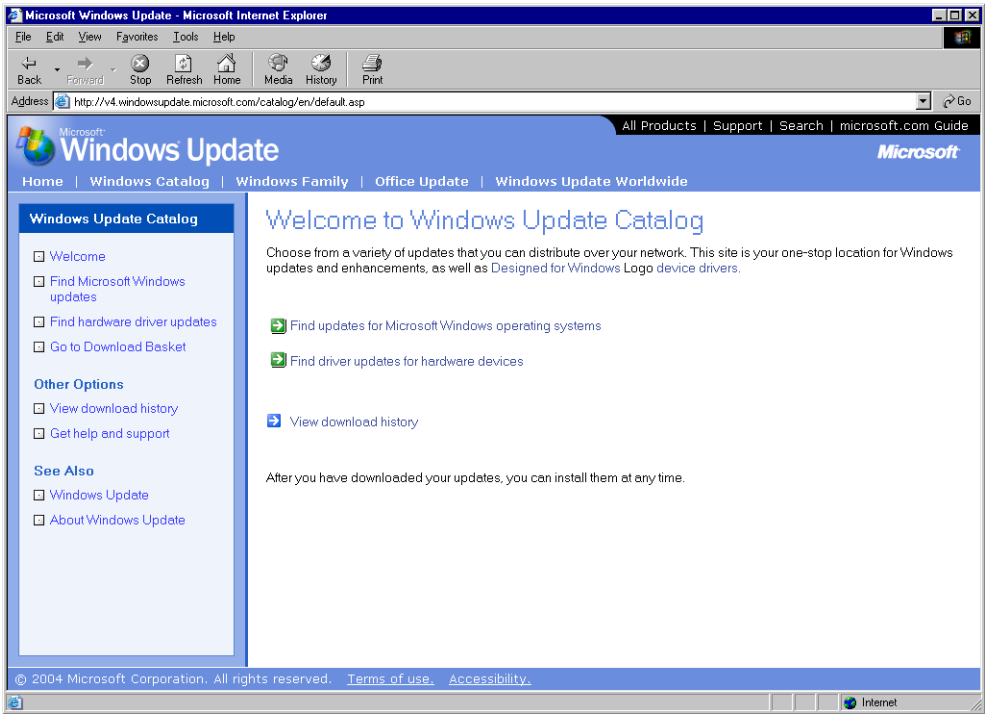
Kuva 3: Ensisijaiset päivitykset

Hakutuloksia tarkasteltaessa voidaan havaita Microsoft Update -palvelun saaneen Windows Update -sivuston kolmen päivitysluokan lisäksi uusia päivitysryhmiä, jotka on eritelty tuotteen mukaan. Esimerkiksi apukirjastojen ja kehitystyökalujen päivitykset löytyvät omasta ryhmästään. Microsoft Update -palvelun kautta ei voi ladata päivityksiä Windows 9x sarjan käyttöjärjestelmille, vaan selain ohjataan automaattisesti Windows Update -sivustolle.

2.3.5 Windows Update Catalog (WUC)

Windows Update Catalog on Microsoftin verkkosivusto, jota voisi kuvailla Windows Update -palvelun itsepalveluversioksi. Päivitysluettelosta löytyvät päivitykset pitää poimia käsin ”ostoskoriin”, josta ne lopulta ladataan tietokoneelle. Asentaminen jää lataajan harteille, mutta paras syy päivitysluettelon käytölle onkin päivitysten kerääminen toisille koneille, jotka eivät jostain syystä pääse suoraan käsiksi Windows Update -sivustoon tai haluttaessa välttää samojen päivi-

tysten lataamista erikseen jokaiselle koneelle. Ladatut päivitykset voidaan polttaa CD:lle tai laittaa jakoon lähiverkossa, jonka jälkeen ylläpidon ongelmaksi jääkin enää arvailla missä järjestyksessä ne olisi optimaalisinta asentaa. Osa uudelleenkäynnistystä vaativista päivityksistä nimittäin sallii toiminnon lykkäämisen ja antaa asentaa muitakin päivityksiä, mutta toiset päivitykset vain sanovat koneen käynnistyvän nyt uudelleen ja antavat asentajalle vain Ok-napin painettavaksi. Pidemmän päälle ylläpitäjästä alkaa tuntua ettei hän voi välttyä tarpeettomilta käynnistyksiltä ja toivoisi voivansa ladata päivityskatalogin kautta saaduille päivityksille myös automatisoidun asennusjärjestelmän.

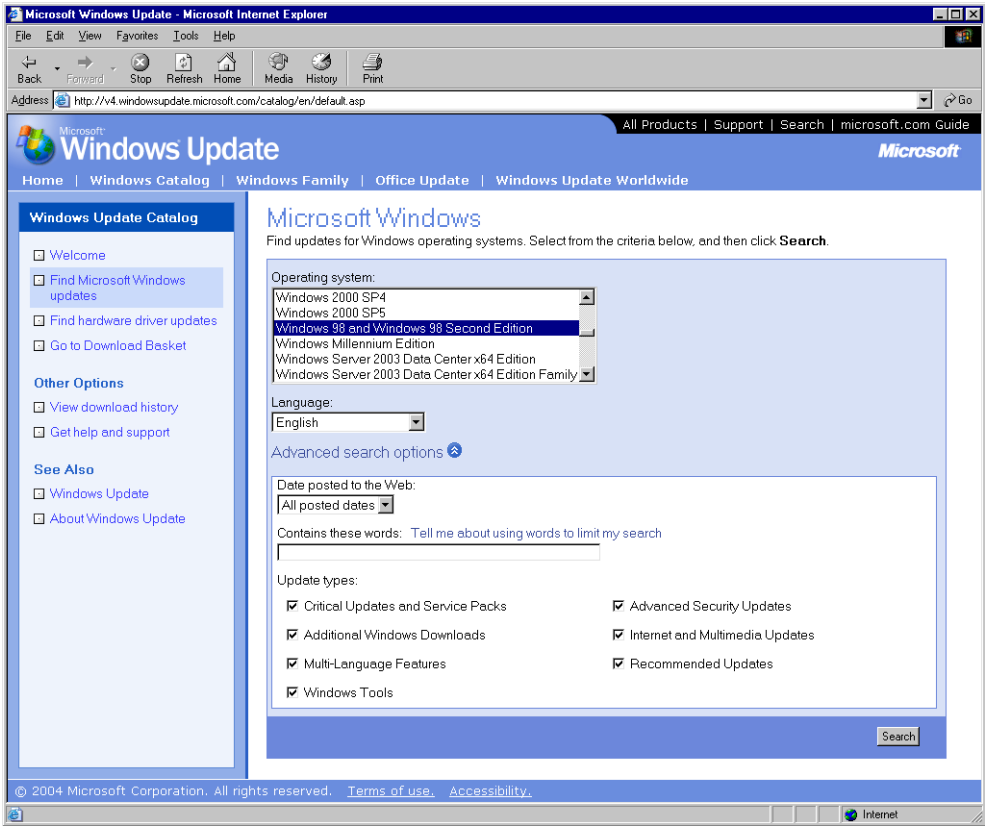


Kuva 4: Windows Update Catalog, pääsivu.

WUC -sivusto on yhä olemassa, mutta kaikki vähänkään uudemmilla Windows-versioilla tehdyt yritykset päästä käyttämään sitä ohjautuvat automaattisesti uudemmalle Microsoft Update Catalog -sivustolle. Niinpä seuraavia kuvakaappauksia varten jouduttiin ottamaan käyttöön vanha kunnon Windows 98 SE.

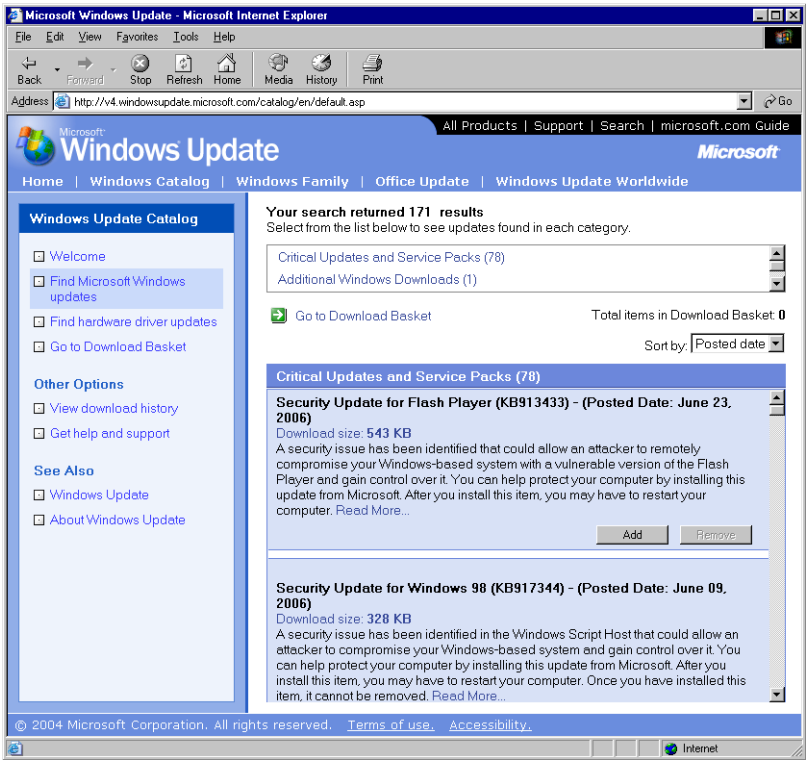
Päällisin puolin WUC muistuttaa paljon WU ja MU sivustoja. Sen kautta vain ei tehdä suoria asennuksia, vaan käyttäjä määrittää itse mitä päivityksiä hän näkee koneidensa tarvitsevan. Lisäksi myös WUC vaatii IE-selaimen käyttöä, vaikka se voisi periaatteessa toimia muillakin selaimella. Päivitysten hakeminen aloitetaan valitsemalla listasta käyttöjärjestelmä ja viimeisin siihen asennut korjauspaketti eli Service Pack., Tällöin käyttäjälle tarjotaan vain sen jälkeen ja en-

nen seuraavaa korjauspakettia ilmestyneet päivitykset. Päivittäminen kannattaisi kuitenkin yleensä aloittaa lataamalla ja asentamalla ensin tuorein SP. Seuraavaksi valitaan haluttu kieli ja jos tarpeen, voidaan hakua vielä tarkentaa itse määritetyillä sanoilla tai valmiina annettujen ryhmien mukaan valitsemalla Advanced Search Options.



Kuva 5: WUC, päivitettävän käyttöjärjestelmän valinta ja hakuehtojen määritys.

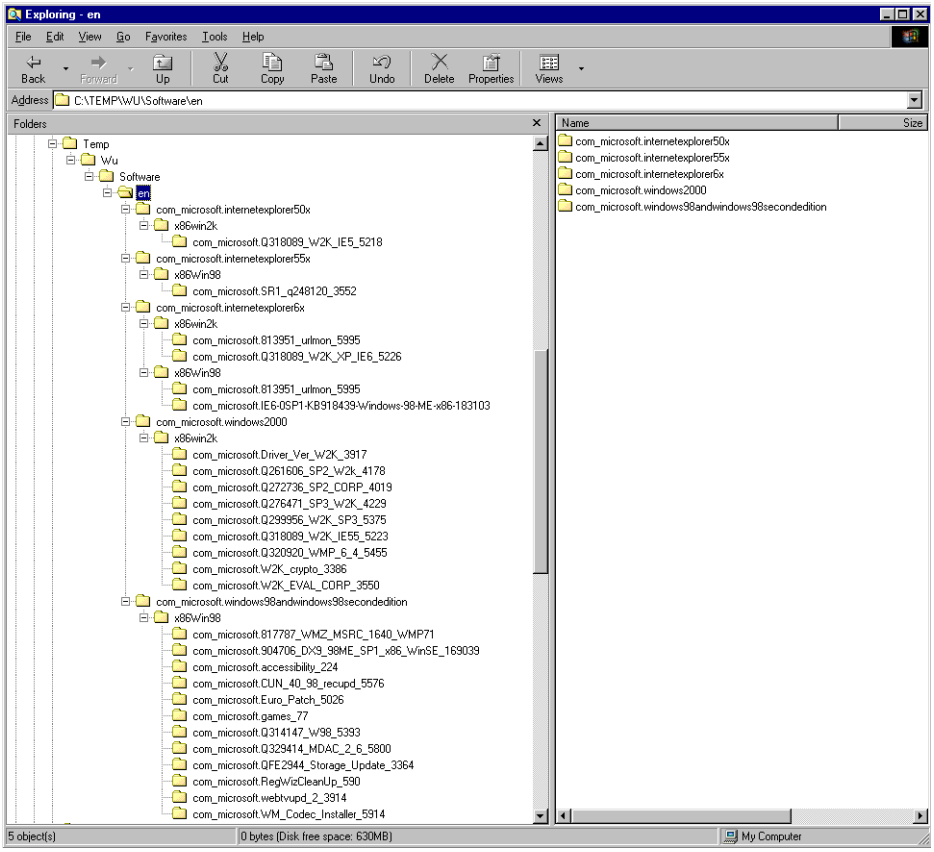
Kuvasta 5 voidaan havaita sivuston tarjoavan päivityksiä myös Windows 2000:n viidennelle korjauspaketille, vaikka Microsoft perui sen julkaisun jo vuonna 2004. Lisäksi listasta puuttuu mm. ”Windows XP SP3” -rivi. Tästä voitaneen päätellä, ettei vanhan päivitysluettelon ylläpito ole enää aivan ajan tasalla, mikä on sääli, sillä WUC olisi käytettävyydeltään huomattavasti sen seuraajaa Microsoft Update Catalog -palvelua toimivampi. Monipuolisten rajausmahdollisuuksien ansiosta käyttäjän silmille ei pitäisi tulvahtaa useita satoja päivityksiä, vaan saadut osumat jaksaa jopa käydä ajatuksen kanssa läpi. Etenkin päivitysten rajaaminen viimeisimmän asennetun korjauspaketin perusteella mahdollistaa vanhentuneiden päivitysten asentamatta jättämisen.



Kuva 6: WUC, kriittiset päivitykset.

Hakutulokset esitetään jaoteltuina samoihin ryhmiin kuin niitä pystyi hakua tehdessä rajaamaankin. Valitsemalla jonkin näistä ryhmistä niiden listauksen alle avautuu linkki latauskoriin, päivitysten järjestysvalikko ja listaus valittuun ryhmään kuuluvista päivityksistä kuvauksineen. Päivityksen kuvauksen alta löytyy napit sen lisäämiseksi latauskoriin sekä myös poistonappi. Ryhmien listaus on tehty melko ahtaaksi eikä niitä siksi voi nähdä kuin vain kaksi kerrallaan. Onneksi palvelu ei kuitenkaan aukea erilliseksi ikkunaksi jonka koko on esim. lukittu 640x480 -näyttötilaan sopivaksi.

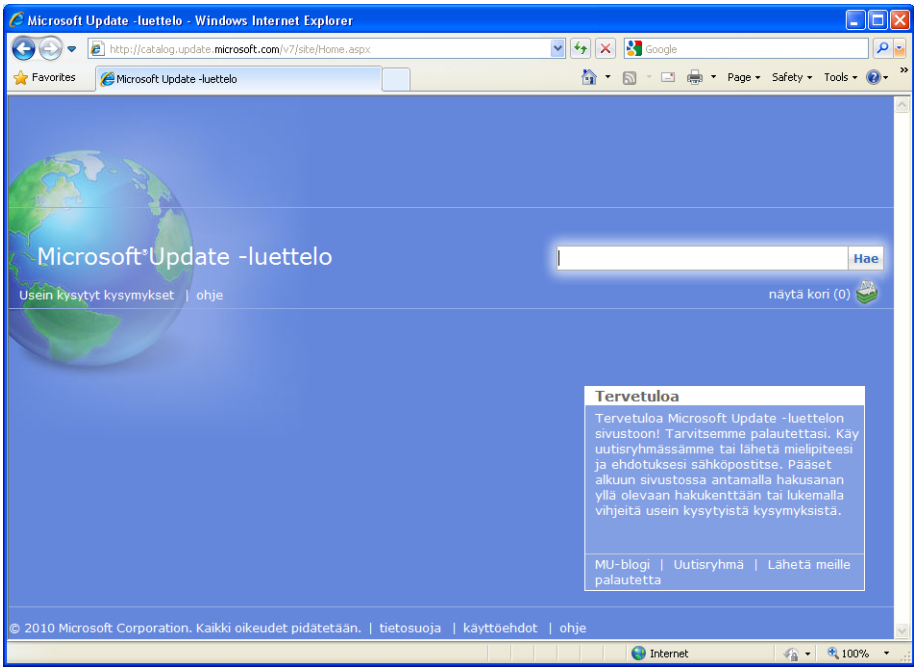
Valittuaan haluamansa päivitykset käyttäjä voi joko tehdä uuden haun esim. toiselle kielelle tai Windows-versiolle tai siirtyä päivitysten lataamisvaiheeseen. Tällöin käyttäjä määrittää haluamansa kohdekansion, jonka alle ladatut päivitykset tallennetaan. Kohdekansio on kuitenkin vain alkupiste moniportaiselle kansiopolkujen kokoelmalle, sillä päivitykset tallennetaan sen alle omiin kansioihinsa.



Kuva 7: WUC, ladattujen päivitysten kansiorakenne.

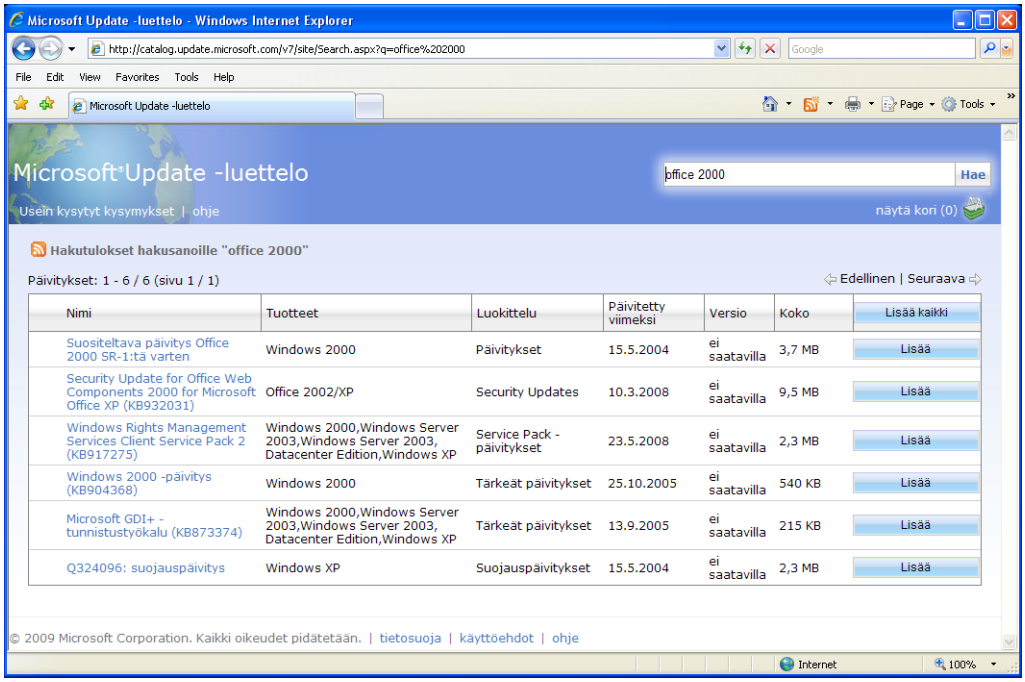
Kuvasta 7 nähdään miten ladatut päivitykset ryhmitellään annetun kohdekansion alle. Kansioiden nimeämiskäytäntö ei välttämättä ole kaikkein optimaalisin omin käsin päivittämistä ajateltuna, sillä yksittäiset päivitykset on eriytetty omiin alikansioihinsa ja esim. IE-selaimen versiot on kansioitu erikseen käyttöjärjestelmäkohtaisista päivityskansioista. Tämän johdosta päivitysten ajojärjestyksen arvailun lisäksi tulee päivittäjän myös kahlata edestakaisin kansioiden välillä. Asennuksen voi tietysti yrittää automatisoida laatimalla skriptin, missä annetaan jokaisen ajettavan päivityksen polku ja perään laitetaan valitsin, joka estää uudelleenkäynnistyksen. Tämä vaatii kuitenkin myös oman vaivansa, kun käyttäjä joko kopioi lataamansa päivitykset yhteen kansioon tai kopioi jokaisen päivityksen polun yksi kerrallaan skriptiinsä. Lisäksi uudelleenkäynnistysten välttelemisestäkin voi koitua käynnistelyä suurempi vaiva, kun jokin päivitys vahingossa korvaa tärkeän tiedoston vanhemmalla tai eri arkkitehtuurille tarkoitetulla versiolla. (Microsoft, 2007.)

2.3.6 Microsoft Update Catalog (MUC)



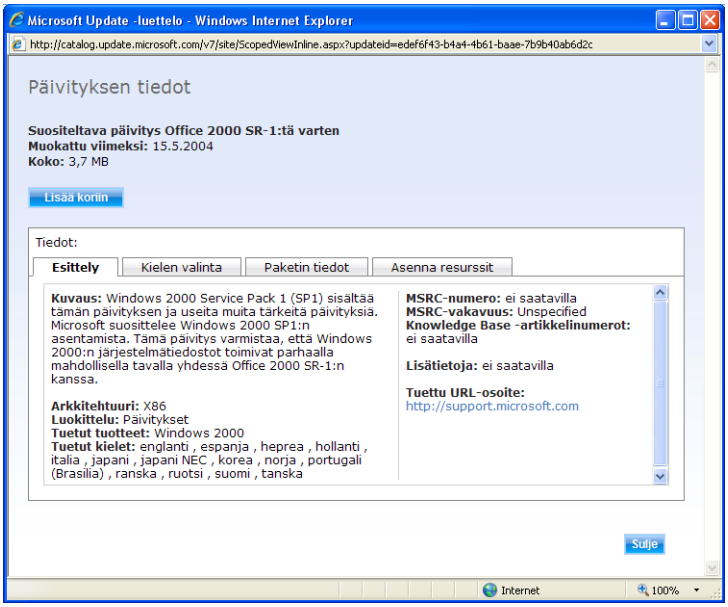
Kuva 8: MUC, pääsivu.

Microsoft Update Catalog (http://catalog.update.microsoft.com/v7/site/Home.aspx) on Windows Update Catalog palvelun seuraaja. Toisin kuin lähes identtiset palvelut WU ja MU, MUC eroaa huomattavasti edeltäjästään, sillä sen ulkonäköä ja käyttöliittymää on virtaviivaistettu niin pitkälle, että seuraavassa vaiheessa siinä varmaankin olisi enää vain yksi iso nappi jossa lukisi ”Lataa kaikki”. MUC tarjoaa käyttäjälle pelkän hakurivin, johon käyttäjän on itse syötettävä haluamansa ohjelmiston nimi ja versio. WUC-sivuston listalta olisi käyttäjä voinut valita esim. prosessorityypin mukaiset päivitykset, kun MUC tarjoaa esim. hakusanoilla ”Windows Server 2003” yli 1000 x86, Itanium ja x64 prosessoreille tarkoitettua päivitystä. Lisäämällä hakuun ”x86” osumia onkin vain 25. Sivuston pelkistetystä ulkoasusta on myös jäänyt pois linkki yksityiskohtaisen haun tekemiseen eikä esim. ”-” merkki hakusanan edessä rajaa sanaa pois, vaan ”-x64” listaakin pelkät x64-päivitykset. WUC-palvelussa valittiin ensin Windows-versio tai muu Microsoftin ohjelmisto ja sen jälkeen valittiin mille kielelle päivitykset haettaisiin. (Oulun yliopiston tietohallinto 2006.)

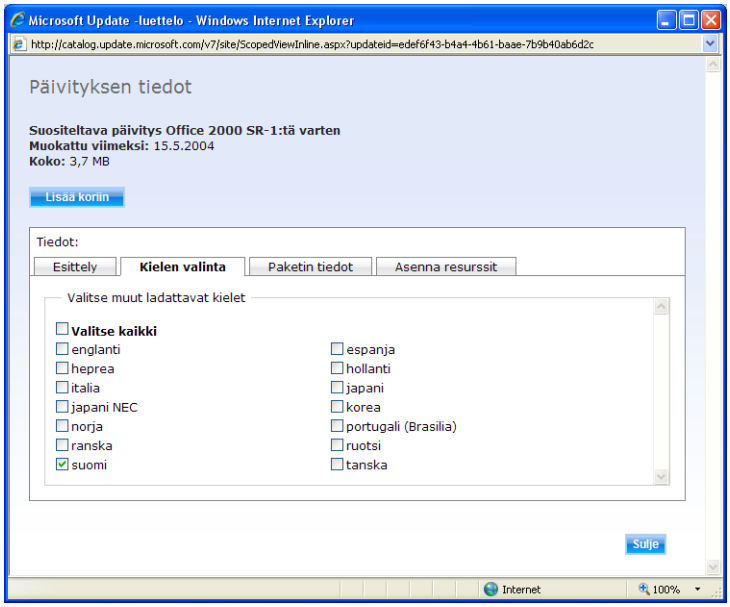


Kuva 9. Microsoft Update Catalog:n esittämä hakutulos.

MUC vaikuttaa myös antavan osumia, jotka eivät näytä vastaavan annettuja hakusanoja. Tämä mutkistaa päivitysten hakua entisestään, kun käyttäjän pitää ottaa selvää onko kyseessä virheellinen osuma vai vajavainen päivityksen kuvaus.

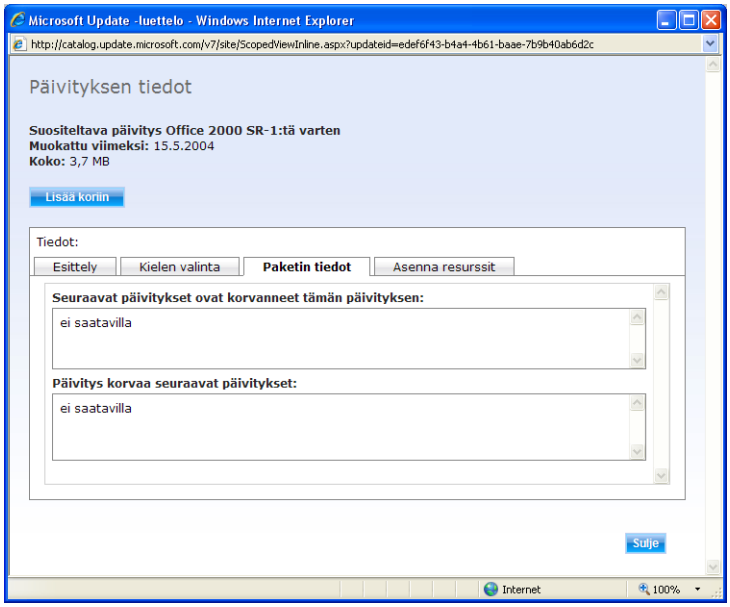


Kuva 10: MUC, päivityksen esittely.

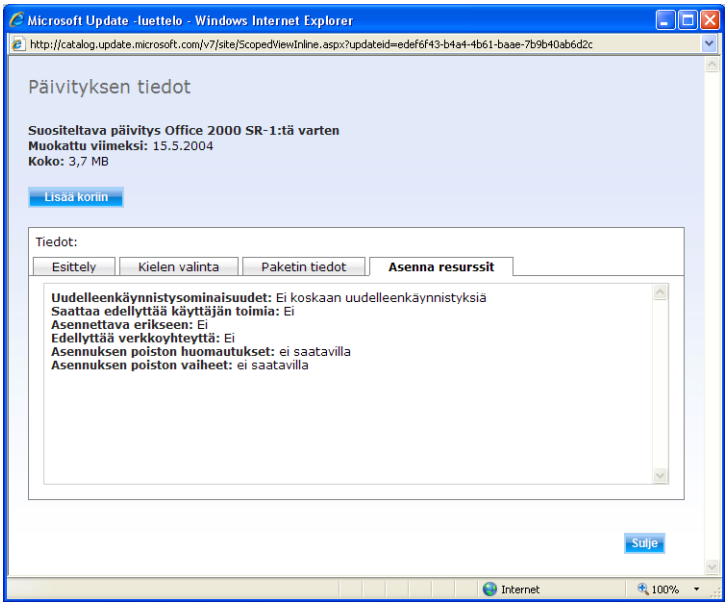


Kuva 11: MUC, valitaan millä kielillä päivitys ladataan.

MUC on ostoskorissaan antavinaan käyttäjän vielä muuttaa ladattavia kieliä, mutta muutokset eivät kuitenkaan tallentuneet. Niinpä käyttäjän harteille jää muistaa valita erikseen oikeankieliset päivityspaketit jokaisen päivityksen kohdalla jo ennen koriin lisäämistä tai päivitysten kerääminen menee vielä työläämmäksi.



Kuva 12: MUC, päivityspaketin tiedot.



Kuva 13: MUC, päivityksen asennukseen liittyvät tiedot.

Kuten WUC, myös MUC toimii vain Internet Explorer -selaimen kautta, mutta toisin kuin WU ja MU, jotka selvittävät ActiveX-komponentin avulla mitä käyttäjän kone on syönyt, Catalog-palvelut voisivat periaatteessa toimia millä selaimella tahansa, koska käyttäjä määrittää täysin itse mitä päivityksiä hän sieltä haluaa ladata sen sijaan, että selaimen kautta nuuskittaisiin mitä juuri sille koneelle pitäisi asentaa.

Siinä missä WUC vielä aikoinaan vaikutti jotenkin hallittavissa olevalta joskin erittäin työläältä tavalta hankkia ja asentaa päivitykset Windows-työasemille, on MUC-sivuston virtaviivaistettu käyttöliittymä tehnyt siitä todella hankalan ja vaivalloisen palvelun.Tästä on helposti luettavissa hienovarainen kehotus siirtyä käyttämään joko automaattisia päivityksiä tai WSUS- ja SMS-palvelinten kaltaisia ratkaisuja.

MUC-palvelun kautta ladatut päivitykset voidaan myös periaatteessa jakaa yrityksen koneille automaattisesti aktiivihakemiston kautta, mutta menetelmä ei itsessään tarjoa mitään palautetta asennusten onnistumisesta ja siten vaatisi esim. Microsoft Baseline Security Analyser -ohjelman avulla kerättyjen listausten seuraamista. Eri käyttöjärjestelmiä ja ohjelmistoversioita käyttävät koneet olisi myös ryhmiteltävä tarkkaan omiin ryhmiinsä aktiivihakemistossa, jotta niille ei yritettäisi väkisin asentaa vääriä päivityksiä. Näistä seikoista johtuen MUC & AD & MBSA yhdistelmä ei kykene kilpailemaan esim. automaattisten päivitysten jakelujärjestelmää hyödyntävien ohjelmiston kanssa.

2.4 Palvelimelta käsin hallitut päivitysten jakeluratkaisut

Suuren työasemamäärän takia on yrityksissä käytännöllisintä jakaa päivitykset omalta palvelimelta, jolloin ylläpito voi päivitysjärjestelmän käyttöliittymän kautta itse valikoida mitä päivityksiä asennetaan millekin koneelle tai ryhmälle ja mihin aikaan asennukset tehdään. Koneiden ryhmittely mahdollistaa päivitysten asentamisen myös eri vaiheissa, antaen ylläpidolle aikaa havaita ja toimia ennen kuin ongelmallinen päivitys on asentunut kaikkiin työasemiin. Järjestelmästä riippuen ei työasemien luokse ihannetapauksessa edes tarvitse jalkautua kuin vain todellisissa vikatilanteissa. Päivityspalvelinkin voidaan ottaa käyttöön ja määrittää työasemat sen alaisuuteen käymättä säätämässä jokaista konetta erikseen esim. Aktiivihakemiston (AD) avulla.

2.4.1 Software Update Services (SUS)

Ennen WSUS-ohjelmiston julkaisua Microsoftin tarjoama ilmainen ratkaisu yrityksen omalta palvelimelta käsin jaettaville päivityksille oli Software Update Services (SUS), jonka tuki lakkautettiin 10.7.2007 (Informationweek, 2006). SUS-palvelun oli asennettavissa Windows 2000 Server ja Windows Server 2003 palvelimille, joihin oli asennettu Internet Information Services (IIS). SUS-palvelimelle ladattiin kaikki tarpeellisiksi koetut Microsoftin jakamat päivitykset ja työasemat ohjattiin hakemaan ne siltä määrittämällä niissä automaattisten päivitysten palvelu käyttämään SUS-palvelinta. Pystyttämällä useamman SUS-palvelimen voitiin yhdestä tehdä pääpalvelin, joka jakoi lataamansa päivitykset alemmille palvelimelle. (Kivimäki 2005a, 257-258.)

SUS ei kuitenkaan tarjonnut ylläpidolle kunnollista tapaa seurata päivitysten asentumista työasemille, vaan sitä varten oli ladattava palvelimelle erillinen työkalu kuten vaikkapa SUS Reporting Tool (Klemencic 2003). SUS-palvelimen IIS-palvelun lokista saa parhaimmillaankin selville vain mitkä päivitykset mikäkin kone on ladannut, joten asennusten onnistumisen selvittäminen vaati vielä esim. MBSA-ohjelman käyttöä.

2.4.2 Windows Server Update Services (WSUS)

WSUS on SUS-palvelimen korvaava ratkaisu, jonka avulla voidaan päivittää Windowsin eri versioiden lisäksi myös muitakin Microsoftin ohjelmistoja ja tuottaa raportteja työasemien päivitystarpeista. WSUS on tarkoitettu kattamaan päivitystarpeet pelkän Microsoft Update -sivuston ja täyden SMS-palvelinratkaisun välillä, eli kourallinen työasemia voidaan päivittää vielä MU-palvelun kautta ja SMS sopii hallinnoimaan useista sadoista jopa tuhansia koneita kattavia verkkoja. WSUS voidaan kuitenkin venyttää palvelemaan jopa yli 10000 työaseman verkkoa. (Kivimäki 2005a, 268; Järvinen 2006, 32.)

Microsoft tarjoaa WSUS-palvelimen käyttöönottoa harkitseville luettavaksi kattavan oppaan ”Deploying Microsoft Windows Update Services”, johon suurimmalta osin tämän kappaleen tiedot pohjautuvat. Oppaasta on myöhemmin julkaistu uudempi versio ”Deploying Microsoft Windows Update Services 3.0 SP1”, joka eroaa edeltäjästänsä mm. hiukan muuttuneilla ennalta asennettavien apuohjelmien vaatimuksilla. (Microsoft 2005, 27 ja Microsoft 20008, 28.)

WSUS on päivitysten hallintaan tarkoitettu ohjelmisto, jonka avulla voidaan hakea päivityksiä Microsoftin päivityspalvelimelta ja varastoida ne omalle WSUS-palvelimelle. Työasemat voidaan ohjata hakemaan päivityksensä tältä palvelimelta tai sen alle määritetyiltä apupalvelimilta. Tämä tapahtuu määrittämällä niille automaattisten päivitysten palvelimen osoite uudelleen joko konekohtaisesti paikallisella käytännöllä tai hyödyntämällä aktiivihakemiston ryhmäkäytäntöjä.

WSUS-palvelimen käyttöön liittyvien asetusten määrittäminen ryhmäkäytäntöjen kautta on sitä suositeltavampaa mitä enemmän ylläpidettäviä koneita yrityksellä on, sillä niiden avulla saadaan esim. WSUS-palvelimen verkko-osoitteen muutos vaivattomasti tiedotettua työasemille. aktiivihakemiston puolella voidaan myös jakaa työasemat erillisiin ryhmiin ja määrittää niille tarpeiden mukaiset asetukset. Esim. päivitysten asennus voidaan laittaa alkamaan eri aikaan tai antaa jollekin käyttäjäryhmälle vapaus ja vastuu päättää milloin oman koneensa päivittävät.

Yrityksen työasemien näkökulmasta WSUS-palvelimen voitaisiin sanoa näkyvän niille ikään kuin Microsoftin omana päivityspalvelimena, ainoana erona onkin vain päivitysvalikoima, jonka laajuus riippuu paikallisen ylläpidon valinnoista. Toisin sanoen työasemien automaattisten päivitysten kyselyt ohjataan WSUS-palvelimelle, joka tarjoaa työasemille ja palvelimille niiden tarvitsemista päivityksistä ne, mitkä ylläpito on ensin hyväksyttänyt.

SUS-palvelinten tavoin WSUS-palvelimia voidaan pystyttää useampia esim. vaikkapa eri paikkakunnilla oleviin toimipisteisiin. Tällöin ne määritetään joko itsenäisiksi palvelimiksi tai ketjutetaan peräkkäin ja hallinnoidaan pääpalvelimen kautta mitä päivityksiä hyväksytään jaettavaksi alipalvelimille. Keskitetyllä hallinnalla mm. voidaan varmistaa ettei jokin päivitys jää epähuomiossa hyväksymättä joltain etäpalvelimelta. Koska ainoastaan WSUS-ketjun ylin palvelin on yhteydessä Microsoftin päivityspalvelimeen, tulee jokainen päivitys ladatuksi ulkoverkosta vain yhden kerran. Pääpalvelimelle ladatut päivitykset voidaan jopa kopioida siirrettävälle medialle ja viedä täysin muusta maailmasta eristettyyn verkkoon pystytetylle WSUS-palvelimelle, joten melkeinpä ainoaksi syyksi käyttää Microsoftin päivityskatalogia jää enää tilanne, jossa ylläpidolla ei olisi käytettävissään kahta Windows-palvelinta joihin WSUS voitaisiin asentaa.

WSUS saadaan pitämään lähiverkon kuormituksen kurissa lataamalla päivitykset ns. Express Installation Files -muodossa. Tämä mahdollistaa työasemille ladattavien päivitysten datamäärän kutistamisen noin kolmasosaan sillä rasitteella, että WSUS-palvelimelle ensin ladataan noin kolme kertaa normaalia isommat päivityspaketit. Normaalikokoisen päivityspaketin sisältämät tiedostot kirjoitetaan vanhojen päälle sellaisenaan, vaikka tiedostojen sisältä pitäisi muuttaa vain muutamaa merkkiä. Express Installation Files -päivityksissä paketit sisältävät ohjeistuksen päivitettävien tiedostojen kaikkien vanhempien versioiden muokkaamiseksi, jolloin yksittäiselle työasemalla ladataan vain sitä koskevat muutokset. Normaalit päivitykset kannattaakin ladata vain mikäli paikallinen operaattori veloittaisi asiakkailtansa kohtuuttoman suuria summia per ladattu megatavu. Silloin kuitenkin esim. eri toimipisteessä olevien työasemien päivittäminen tulisi todella kalliiksi ellei niille pystytettäisi omaa WSUS-palvelinta.

2.4.3 Systems Management Server (SMS)

Aiemmissa kappaleissa käsitellyistä Microsoftin tarjoamista päivitysten asennusratkaisuista poiketen SMS-ohjelmisto itsessään on maksullinen, minkä lisäksi jokaiselle sen palveluja käyttävää työasemaakin kohden on ostettava lisenssi. Hintansa vastineeksi SMS sisältää paljon muitakin toimintoja pelkän päivitystenjakelun lisäksi, mutta toisaalta niihin perehtymiseksi tulisi ylläpidon lukea monen monta opasta kuten esim. Microsoftin julkaisema lähes 700-sivuinen SMS-opas Systems Management Server 2003 Concepts, Planning, and Deployment Guide. Nimensä mukaisesti kyseinen opas keskittyy SMS-palvelinten käyttöönoton suunnitteluun ja toteutukseen, varsinaisen hallinnan opetteluun on sitten omat oppaansa.

Suunnittelun pohjustukseksi opas sentään antaa lukijalleen jonkinlaisen käsityksen palvelun tarjoamista mahdollisuuksista, joista voidaan pelkkien päivitysten jakelun lisäksi mainita mm. työasemien laitteiston ja ohjelmistojen inventointi, ohjelmistojen käyttöasteen seuranta, etähallintatoiminnot, verkon diagnostiikka, raportointityökalut, kannettavien tietokoneiden hallinta, Aktiivihakemisto ja varmuuskopiointi (Microsoft 2003, 2). Ylläpito voi siis mm. saada ennalta selville mitkä työasemat eivät täytä asennettavaksi määrätyn ohjelmiston vaatimuksia, jolloin ne voidaan vaihtaa vaatimukset täyttäviin ennen käyttöönottoa. Tarvittavien ohjelmistolisenssien tarvetta voidaan seurata teettämällä raportteja, joista selviää vaikkapa asennusten tai yhtäaikaisessa käytössä olevien ohjelmistojen määrä. Toimipisteiden välillä liikkuvat läppärit voidaan määrittää päivittymään lähimmän palvelimen kautta ja koko SMS-palveluiden varmuuskopioiden teettämisen sisällyttäminen itse järjestelmään helpottaa merkittävästi niiden hoitamista. (Microsoft 2003, 3-19.)

Microsoftin päivitysten lisäksi SMS kykenee jakelemaan työasemille myös muiden valmistajien ohjelmistoja, mutta se vaatiikin jo huomattavasti syvällisempää perehtymistä asiaan ja kuten oheisesta linkistä voi päätellä, ei se ilmeisesti ole aivan helppoa temppu SMS-veteraaneillekaan: http://www.winbatch.com/whitepapers/sms_package_construction.html. SMS-palvelinten kanssa näyttäisi muutenkin joutuvan naputtelemaan paljon enemmän tai vähemmän monimutkaisia skriptejä, jotta siitä saisi kaiken hyödyn irti. Eräs merkittävimmistä SMS-palvelimen ominaisuuksista, ja mikä osittain kiertää muiden kuin Microsoftin ohjelmistojen jakelun hankaluudet, on SMS OS Deployment Pack, joka mahdollistaa käyttöjärjestelmien asentamisen ja palauttamisen työasemille levykuvien avulla (Savill 2005). SMS 1.0 julkaistiin jo vuonna 1994, sen seuraaja 2.0 ilmestyi vuonna 1999 ja SMS 2003:n piti alunperin olla versio 3.0, mutta se nimettiinkin julkaisuvuotensa mukaan (myITforum.com 2009). Esimerkiksi oppilaitosten luokkien työasemat on käytännössä pakko ”resetoida” säännöllisin väliajoin jo ihan siksi, etteivät oppilaiden lataamat tiedostot lopulta tukkisi koneiden kiintolevyjä. Tämä hoituu mukavimmin verkon kautta toteutettuna massa-ajona käyttäen levykuvaa referenssikoneesta, johon on asennettu kaikki tarvittavat ohjelmistot päivityksineen. Nykyään SMS on jaettu kahdeksi ohjelmistoksi. Näistä System Center Essentials (SCE) on tarkoitettu ns. yhden metsän verkkoon, jossa voi olla maksimissaan 30 palvelinta ja 500 työasemaa, kun taasen System Center Configuration Manager (SCCM) tarjoaa monipuolisemmat ominaisuudet ja tukee paljon laajempia verkkoja.

2.5 Apuohjelmistot

Päivitysten jakelun hallinnointia ja seurantaa varten voidaan palvelimille ja työasemille joutua asentamaan joitakin lisäohjelmistoja ja palveluja, joista osasta on tässä annettu lyhyet kuvaukset. Niitä saatetaan tarvita esim. WSUS-palvelun asennusta varten, helpottamaan koneryhmien hallintaa tai tarjoamaan tietoa työasemien tietoturvariskeistä.

2.5.1 Microsoft Baseline Security Analyser (MBSA)

MBSA on Microsoftin tarjoama tarkistusohjelma, jolla voidaan tarkistaa onko testatun koneen tietoturva ajan tasalla. Ohjelma pystyy myös yhdeltä koneelta käsin tarkistamaan muutkin lähiverkon koneet ja se raportoi mm. keskenjääneistä asennuksista ja tarjoaa linkit puuttuvien päivitysten lataamista varten. (Järvinen 2006, 29-31.)

2.5.2 Active Directory (AD)

AD eli aktiivihakemisto on Microsoftin toteutus hakemistopalvelusta. Hakemistosta hakemistopalvelu eroaa siinä, että hakemiston tietojen lisäksi se tarjoaa myös palvelut niiden käsittelyyn (Kivimäki 2005b, 1). Tietokone- ja käyttäjätilit säilötään organisaatioyksiköihin (Organization Unit, OU), joihin voidaan puolestaan kohdistaa ryhmäkäytäntöjä (Group Policy Objects, GPO) määrittelemään esim. ohjelmien automaattisia asennuksia ja salasanakäytäntöjä. Tietokone- ja käyttäjätilit voidaan jakaa tarpeen mukaan useampiin alempiin organisaatioyksiköihin. Tällöin ylemmän yksikön käytännöt voidaan periä alemmille yksiköille (Kivimäki 2005b, 7; 371; 527). Graafisesti OU:t esitetään kansioina ja niiden sisältämät objektit voitaisiin nähdä tiedostoina. Yksiköille voidaan ominaisuuksien puolella lisätä yksi tai useampi GPO. Käytännöillä voidaan esim. estää taustakuvan vaihtaminen sekä määrittää mihin aikaan halutuilla käyttäjätileillä voidaan kirjautua työasemille. Vastaavat toimenpiteet onnistuvat myös työasemien paikallisten käytäntöjen kautta, mutta silloin myös muutokset joudutaan tekemään työasemakohtaisesti.

3 Empiirinen osuus

Päivitysjärjestelmän pystytyskohteena toimiva yritys on yksi Suomen suurimpia perheyrityksiä työllistäen vajaat tuhat henkeä ympäri Eurooppaa, joista yli puolet työskentelee Suomessa. Yli kuusikymmenvuotias yritys valmistaa tuotteita rakennusteollisuuden ja kaupan käyttöön. Yhtiön pääkonttori sijaitsee Helsingissä ja sen myynnistä noin kolmannes kohdistuu Suomeen.

3.1 Lähtötilanne

Aiemmin yrityksen tietokoneiden on täytynyt hakea tietoturvapäivitykset automaattisesti suoraan Windows/Microsoft Update -sivustolta. Ratkaisu on toiminut sinänsä hyvin niiden koneiden osalta, joilla on toimiva nettiyhteys yrityksen intranetin ulkopuolelle ja joilla ei ole mitään erityistä syytä jättää jonkin tyyppiset päivitykset asentamatta. Esimerkiksi joidenkin automaattisesti täytettävien tulostepohjien kanssa on havaittu, ettei kaikkia Microsoftin Office-tuoteperheen päivityksiä välttämättä tulisikaan asentaa tulostuksesta vastaaviin koneisiin ellei ole valmis käymään jokaista pohjaa läpi ja varmistaa, että tiedot osuvat yhä kohdalleen. Päivityksiä ei tietenkään ole pakko määrittää asentumaan automaattisesti, mutta silloin ne pitäisi muistaa ja ehtiä ajaa käsin heti joka päivitystiistain jälkeen. Jotta ongelmalliset päivitykset jäisivät asentamatta kriittisemmissä työasemissa, tulisi näiden koneiden osata olla asentamatta niitä ja siksi käyttäjille pitäisi antaa riittävät oikeudet päivitysten ajamiseen käsin. Kannettavien koneiden ja toimiston työasemien kanssa tämä vielä voisi toimia, koska niiden haltijoilla voidaan olettaa olevan henkilökohtaiset intressit pitää omat koneensa kunnossa, mutta tuotannon käytössä olevilla työasemilla on jo vuorotyön takia niin monta isäntää, että on parempi jättää päivitysten asentaminen ylläpidon harteille.

Tuotannon työasemilta ei ole tarkoitus päästä surffaamaan nettiin, mutta samalla on tullut suljettua myös Microsoftin päivityssivustot pois käytöstä. Näille koneille on ylläpidon toimesta ajettu päivityksiä konekohtaisesti aina kun vain on ollut aikaa käydä määrittämässä työasemalle yhteys nettiin, valvoa vieressä päivittämisen etenemistä ja lopuksi palauttaa verkkoasetukset normaaleiksi. Nämä työasemat myös sijaitsevat mikä missäkin päin tuotantotiloja, kun taas toimistokoneet löytyvät toistensa läheltä. Lähekkäin sijoitettujen työasemien päivittämisen voisi vielä hoitaa yhdessä illassa per kuukausi ”rinnakkain”, laittamalla ne kaikki päivittymään peräkanaa ja kiertää sitten käynnistämässä ne tarvittaessa uudelleen ja lopulta tarkistaa niiden sammuneen. Etähallinnalla tätä tietysti voisi yrittää myös tuotannon koneilla, mutta tuotanto

toimii sekä kahdesta että kolmessa vuorossa ja viikonloppuna tehtynä etähallinta päätyy kuitenkin patikoinniksi viimeistään siinä vaiheessa, kun jokin päivitys jumittaa muutaman koneen tai peräti saa Windowsin palomuurin heräämään estämään etäyhteydet. Vaikka kannettavien tietokoneiden haltijoilla onkin paremmat valmiudet ja motivaatio hoitaa itse päivitysten valikointi ohjeiden mukaisesti, ylläpidolla olisi hyvä olla keinot seurata ovatko päivitykset muistettu tai ehditty aina asentaa vai onko kiireessä automaattisten päivitysten muistutus klikattu tottumuksesta pois näkyvistä.

Kaiken kaikkiaan yrityksellä on Suomessa jo yli 200 tietokonetta kahdessa toimipisteessä ja luku vain kasvaa ajan myötä. Näistä lähes kaikissa työasemissa on käytössä Windows XP, joitakin Windows 2000 -koneita on vielä pyörittämässä muutaman arvokkaan instrumentin hallintaohjelmistoa. Vaikka Windows 95 on jo antiikkia, on sitäkin käytetty yhä muutamassa koneessa kunnes niissä pyörivät ohjelmistot ja niiden ohjaamat järjestelmät uusitaan. Kaikissa työasemissa olisikin jo Windows XP elleivät joidenkin oheislaitteiden ja järjestelmien uudempia käyttöjärjestelmiä tukevat ohjelmistopäivitykset vaatisi kalliita lisenssimaksuja tai peräti koko laitteen uusimista. Yrityksessä onkin laskettu tulevan edullisemmaksi säilyttää varastossa vanhoja työasemia varakoneina jotka sitten parhaimmassa tapauksessa voidaan sellaisenaan ottaa suoraan käyttöön vikatilanteen yllättäessä. Näin oheislaitteet tarvitsee uusia vasta kun niiden oma elinkaari lähestyy loppuaan. Tavallisten työasemien lisäksi yhä useammasta sähkökaapista saattaa löytyä logiikan lisäksi myös teollisuus-PC, jossa pyörii Windows CE, 2000 tai XP. Palvelimissa pyörii mm. Windows 2000 Server ja Windows Server 2003.

3.2 Esivalmistelut

Ennen yhteydenottoa kohdeyritykseen selvitettiin pääpiirteittäin millaisia vaihtoehtoja päivitysten hallinnoidulle jakelulle on saatavissa ja mitä resursseja niiden käyttöönotto vaatii. Työvaiheista tehtiin alustavaksi toteutussuunnitelmaksi seuraavanlainen lista:

- Viitemateriaaliin tutustuminen. Kohdeyrityksen tarpeiden ollessa tiedossa niiden pohjalta rajataan toteutuskelpoisimmat vaihtoehdot ja tutustutaan tarkemmin niistä löytyvään lähdeaineistoon, jonka pohjalta valitaan testaukseen otettava järjestelmä. Saatujen tietojen mukaan päätetään voidaanko testaus toteuttaa olemassa olevalla laitteistolla vai tarvitaanko siihen oma palvelin.
- Testiympäristön pystytys, laitteiden verkotus ja hallinta. Selvitetään millä laitteistolla ja missä keskitettyä päivitysten jakelua voidaan testata sekä miten niiden verkotus ja hallinta toteutetaan. Testikoneet ja -verkko pystytetään ja työasemiin asennetaan päivitysjärjestelmän piiriin kuuluvat ohjelmistot. Koneista otetaan levykuvat joista ne voidaan palauttaa alkutilaansa nopeasti jotta niissä voidaan ajattaa samat päivitykset niihin useaan otteeseen.
- Palvelimen pystytys ja ohjelmistojen asennus. Päivityspalvelimeksi valittuun tai hankittuun koneeseen asennetaan tarpeelliset perusohjelmistot, jonka jälkeen siitäkin otetaan levykuva talteen. Päivitystenjakeluohjelmisto asennetaan ja otetaan uusi levykuva, jotta järjestelmän voi asetuksiin tehdyt voidaan tarvittaessa peruuttaa.
- Testikoneiden liittäminen palvelimen alaisuuteen. Työasemat määritetään päivittymään annetun päivityslähteen kautta. Tarkempi toteutus riippuu valitusta järjestelmästä, mutta käytännössä se tehdään joko työasemille asennettavan asiakasohjelman avulla tai käskyttämällä koneita keskitetysti esim. aktiivihakemiston kautta.
- Päivitysten valinta ja hallinta. Määritetään mitä päivityksiä halutaan ladata työasemien asennettavaksi ja missä niitä varastoidaan, lisäksi päätetään mihin aikaan päivitykset asennetaan ja miten koneiden tulisi käyttäytyä esim. päivitysten vaatiessa uudelleen käynnistystä.
- Testaus, toistot. Aluksi tarkastellaan saadaanko koneet päivittymään sellaisenaan vai pitääkö niitä paljonkin avittaa aluksi jotta automaattinen päivittyminen alkaa toimia. Vaadittujen toimenpiteiden monimutkaisuudesta riippuen voidaan esim. esittää, että uudet työasemat päivitetään käsin uusimman korjauspaketin tasolle ennen päivitysjärjestelmän alaisuuteen liittämistä. Perustoiminnallisuuden varmistuttua aloitetaan päivityksien

ajaminen testikoneisiin, minkä jälkeen koneet palautetaan levykuvista lähtötilanteeseen ja aloitetaan päivityskierros uudelleen. Mikäli useamman toiston jälkeenkin järjestelmä vaikuttaisi toimivan riittävän hyvin, voidaan siirtyä käyttöönottovaiheeseen.

- Käyttöönotto. Olettaen että päivitysjärjestelmässä ei esiinny testauksen aikana kohtuuttomia ongelmia, valittu päivitysjärjestelmä otetaan laajempaan käyttöön vaiheittain. Aluksi järjestelmän piiriin voidaan lisätä sitä fyysisesti lähimpänä sijaitsevat työasemat, sitten saman toimipisteen kaikki työasemat. Lopuksi järjestelmä siirretään testitiloista yrityksen palvelinhuoneeseen ja sen alaisuuteen liitetään loputkin koneet. Ylläpidolle annetaan ohjeistus järjestelmän käytöstä ja työasemat ryhmitellään esim. tuotannon ja toimiston koneisiin. Järjestelmän käyttöönotosta annetaan tiedotteita työnjohdolle ja toimihenkilöille sitä mukaa kuin työasemia siihen liitetään.
- Seuranta ja raportointi. Mahdollisten ongelmien varalta päivitysjärjestelmän toimintaa seurataan tarkkaan seuraavien kuukausien aikana. Samalla laaditaan yhteenveto sen käyttöönotosta sekä tehdään tarkemmat käyttöohjeet yrityksen ylläpidolle.

Lista toimi pohjana varsinaiselle toteutussuunnitelmalle, kun kohdeyrityksen tarpeet ja tarjolla olevat resurssit saatiin selville sekä vaihtoehtoisista päivitysratkaisuvaihtoehdoista oltiin luettu riittävästi ja valittu niistä testaukseen sopivin ehdokas.

3.3 Tarpeiden ja resurssien kartoitus

Ennalta laaditun alustavan suunnitelman jälkeen vuorossa oli virallisempi yhteydenotto kohdeyritykseen. Ensin puhelimitse ja lopulta tapaamisten kautta selvitettiin mitä tarpeita ratkaisun tulisi täyttää ja millä resursseilla se voitaisiin toteuttaa. Koska yritys oli ennalta tuttu, sen työasemista ja niiden päivitystilanteista oli jo jonkinlainen käsitys valmiina. Sen sijaan päivitysten paikallisen keskitetyn jakelun toteuttamiseen käytettävissä oleva laitteisto ja aika olivat vielä tässä vaiheessa tuntematon muuttuja. Lisäksi työasemien ryhmittely ja valmiina olevat palvelut kartoitettiin palaverien aikana. Vaikka päivitysten asentelulla voisikin vielä vitsailla olevan varsin työllistävä vaikutus, konekannan kasvaessa tarvittaisiin ennen pitkää palkata joku tekemään sitä päätoimisena työnään ja lopulta hänellekin tarvittaisiin vielä apumies. Jotta yrityksen ATK-osaston kaikki aika ei siis menisi koneiden päivittämiseen, tulisi päivitysprosessi automatisoida niin pitkälle kuin suinkin mahdollista. Käytäessä läpi yrityksen tietoverkon nykytilaa päädyttiin seuraaviin vaatimuksiin, jotka päivitysjärjestelmän tulisi täyttää:

- Kaikkien koneiden oltava päivitettävissä sisäverkon kautta.
- Microsoftin ohjelmistot on saatava päivitettyä, muutkin päivitykset kelpaavat.
- Päivitykset tulee voida testata valituilla koneilla ennen yleiseen jakoon päästämistä.
- Päivitykset on voitava kohdistaa asentumaan vain tietyille työasemille tarvittaessa.
- Päivitysten on pystyttävä asentumaan ilman työaseman haltijan toimia.
- Päivitysten päätteeksi koneet eivät saa käynnistyä itsestään uudelleen.
- Päivitysten asentumisajankohta on voitava määrittää palvelimien kautta.
- Kannetavan tietokoneen haltijan tulee voida ajaa päivitykset silloin, kun hänelle sopii.
- Päivitykset tulee tarvittaessa voida asentaa heti, ohi ajastuksen.
- Ylläpidon tulisi voida seurata miten päivitykset ovat asentuneet työasemiin.
- Vanhentuneet päivitykset tulee voida poistaa palvelimelta.
- Järjestelmä ei saisi kuormittaa verkkoa kohtuuttomasti.
- Järjestelmä ei saa olla erityisen kallis.

Vaatimuslistasta käy ilmi, että päivitysten jakeluun tarvitaan yrityksen sisäverkossa oleva palvelin, jolle päivitykset haetaan Microsoftin palvelimilta. Työasemat tulee voida jakaa ryhmiin ja päivitykset on voitava hyväksyä ryhmän mukaan. Päivitysten asentuminen ei saa kaatua käyttöoikeuksien puutteeseen eivätkä työasemat saaa käynnistyä itsestään uudelleen ilman käyttäjän hyväksyntää. Päivitysten asentumiselle on voitava määrittää ryhmäkohtaisesti haluttu ajankoh-

ta, mutta toisaalta joidenkin ryhmien kohdalla käyttäjillä on oltava valtuudet valita itse milloin heille sopii päivittää työasemansa. Päivitysten on myös tarvittaessa oltava ajettavissa ohi ryhmälle määritetyn ajankohdan. Päivitystenjakeluohjelmiston kautta tulee voida seurata päivitysten tarvetta konekohtaisesti sekä siivota palvelimelle kertyneistä päivityksistä pois uudemmilla versioilla korvatut tiedostot. Jos vain mahdollista, koneille vältetään lataamasta valtavia asennuspaketteja, niin että järjestelmä kykenee toimittamaan yksittäiselle työasemalle vain sille tarpeelliset tiedostot. Eduksi lasketaan myös, jos järjestelmä ei tulisi kohtuuttoman kalliiksi pystyttää ja ettei sen myötä etenkään olisi tarvetta ostaa ”päivityslisenssiä” jokaista siihen liitettyä työasemaa kohden. Eli mieluiten valitaan ilmainen ohjelmisto, tai vähintään ilman toistuvia lisämaksuja.

3.3.1 Käytettävissä olevat resurssit

Päivitysjärjestelmäksi valitun ohjelmiston kustannukset on tarkoitus minimoida. Sen pyörittämiseen tarvittava palvelin kuitenkin hankittiin, jotta päivitysjärjestelmä ei kuormittaisi etenkään testivaiheessa mitään muita tehtäviä hoitavaa palvelinta. Lisäksi järjestelmä haluttiin ottaa käyttöön jo kesäkuun alussa 2008 ja sen testaus ja käyttöönotto hoidettaisiin palkallisena täysiviikkoisena työnä maaliskuun puolivälistä alkaen. Alustavassa suunnitelmassa oli tarkoitus hoitaa testausprosessi kesätöiden yhteydessä, kun kevään jokseenkin tyhjä lukujärjestys olisi ensin hyödynnetty laajemman viitemateriaalin keräämiseen ja siihen perehtymiseen. Yrityksen toiveiden mukaisesti testaus ja käyttöönotto kuitenkin päädyttiin aikaistamaan sillä varauksella, että tiukentuneen aikataulun johdosta eri vaihtoehtojen hyviä ja huonoja puolia ei enää ennätettäisi pohtia niin perusteellisesti. Tämän sijaan keskityttiin varmistamaan, että ennakkosuosikiksi päätynyt järjestelmä todella täyttää vaatimukset. Yrityksen kanssa sovittiin joustavasti työaikajärjestelyistä, jotta muutamat opintopisteet oli mahdollista suorittaa työn ohessa.

3.4 Muokattu toteutussuunnitelma

Alustavan suunnitelman ja palaverien pohjalta laadittiin uusi toteutussuunnitelma, jonka mukaan päivitysjärjestelmä valinta, testaus ja käyttöönotto tultaisiin tekemään. Tässä vaiheessa pystyttiin myös paremmin huomioimaan paljonko aikaa mihinkin tehtävään olisi käytettävissä.

3.4.1 Viitemateriaaliin tutustuminen

Päätös aikaistaa työn aloitus johti siihen, että kaikki käytettävissä oleva aika ennen työpaikalle saapumista ja työn virallista alkamista kohdistettiin valituksi tulleen järjestelmän ohjeistukseen perehtymiseen. Selvitetään ennalta miten päivitysjärjestelmä asennettaan, työasemat liitetään sen alaisuuteen ja kuinka päivityksiä hallinnoidaan. Käytettävissä oleva aika ei kuitenkaan ole helposti arvioitavissa, koska meneillään olevat muut opinnot tuottavat myös tehtäviä suoritettavaksi..

3.4.2 Testiympäristön pystytys, laitteiden verkotus ja hallinta

Työpaikalle saavuttua aletaan kartoittaa missä ja millä laitteistolla testaus tehtäisiin. Lisäksi mietitään kuinka koneita hallitaan ja miten niiden verkotus toteutetaan. Testilaitteisto kasataan käyttökuntoon testaamiselle valitussa tilassa, käyttöjärjestelmäksi asennetaan osaan työasemista Windows 2000 ja loppuihin Windows XP. Kaikkiin työasemiin asennetaan Office 2003, virustorjunta ja vielä lisäksi etähallintaohjelmisto. Service Pack -kokoelmapäivityksiä ei asenneta, vaan ne yritetään asentaa suoraan päivityspalvelimen kautta mikäli suinkin mahdollista. Lopulta työasemista otetaan vielä levykuvat, jotta koneet voidaan palauttaa päivittämättömään tilaan testiajon toistoja varten. Aikaa testiympäristön suunnitteluun ja pystytykseen on käytettävissä noin kaksi viikkoa palvelimen toimitusta odotellessa.

3.4.3 Palvelimen pystytys ja ohjelmistojen asennus

Palvelimen saavuttua siihen asennetaan käyttöjärjestelmä ja virustorjunta. Tämän jälkeen otetaan järjestelmästä levykuva, jotta sekin olisi nopeasti palautettavissa alkutilaansa mikäli jokin menisi tarpeeksi pahasti pieleen ja uudelleenasennus osoittautuisi viisaimmaksi ratkaisuksi. Lopuksi asennetaan itse päivitysjärjestelmä ja otetaan vielä uusi levykuva. Asennusvaiheista ote-

taan kuvakaappauksia muistiinpanojen tueksi ja dokumentoinnin havainnollistamiseksi. Palvelin tulisi saada testivalmiuteen parissa päivässä.

3.4.4 Testikoneiden liittäminen palvelimen alaisuuteen

Määritetään testaukseen valitut työasemat hakemaan päivityksensä testipalvelimelta. Luodaan testiryhmät, joihin koneet kohdistetaan. Mikäli tapoja on useita, pyritään kokeilemaan kaikkia. Aikaa ei kuitenkaan ole tarkoitus haaskata täysin turhien menetelmien testaamiseen, jos toimivampia ratkaisuja löytyy. Määritetään mihin aikaan päivitykset halutaan ajaa testiryhmien koneisiin ja miten niiden tulee toimia päivitysten jälkeen. Koneet on saatava päivitysvalmiuteen parissa päivässä, tarvittaessa niiden ryhmittelyä voidaan muokata testauksen edetessä tarpeen mukaan.

3.4.5 Päivitysten valinta ja hallinta

Opetellaan käytännön tasolla kuinka saatavilla olevista päivityksistä erotellaan tarpeelliset paketit vanhentuneiden ja ei käytössä olevia ohjelmia koskevien joukosta. Tutustutaan kaikkiin päivitysten hallintaohjelmiston valikoihin ja perehdytään käyttöohjeisiin. Jonkinlainen kokonaiskuva tulisi saavuttaa parissa päivässä. Käyttöliittymään totuttelun jälkeen ryhdytään miettimään mitä päivityksiä testikoneille halutaan asentaa ja valitaan niistä osa palvelimelle ladattavaksi.

3.4.6 Testaus, toistot

Kun kaikki esivalmistelut on tehty, voidaan päivitysjärjestelmän toiminnan varsinainen testaus aloittaa. Aluksi kokeillaan kuinka koneet päivittyvät määrättynä ajankohtana. Päivityksiä lisätään palvelimelle muutama kerrallaan sitä mukaa, kun aiemmat ovat testikoneisiin asentuneet. Seuraavaksi kokeillaan kuinka helposti päivityksiä voidaan ajaa ennalta määrätyn aikataulun ohitse. Erilaiset päivitysten ajokäytännöt testataan myös. Kun lopulta kaikki testikoneet on saatu viimeisen päälle päivitettyä, ne palautetaan alkutilaansa levykuvista ja testit ajetaan uudelleen parhaimmiksi todetuilla asetuksilla vielä useaan otteeseen, jotta mahdolliset virhetilanteet voitaisiin havaita. Mikäli tulokset vaikuttavat lupaavilta, voidaan testattavien koneiden kirjoa lopulta laajentaa vähemmän kriittisillä työasemilla jotta varmistuisi, etteivät testikoneiksi päätyneet koneet olleet raudaltaan vain aivan sattumalta poikkeuksellisen yhteensopivia päivitysjärjestelmän kanssa. Mahdolliset toimintaongelmat pyritään ratkaisemaan ja arvioidaan kuinka

usein ne voivat toistua ja paljonko aikaa niiden korjaaminen tulisi viemään. Esim. mikäli muutamasta työasemasta vielä puuttuu jokin päivitys joka mahdollistaa päivitysjärjestelmän kanssa toimimisen, ei vaiva ole kovinkaan suuri verrattuna siihen, että joka toisen koneen kanssa pitäisi käydä paikanpäällä selvittämässä miksi jokin tuoreempi päivitys ei asennu vaikka kaikki muut asentuvat automaattisesti. Uudet koneethan päivitetään ATK-osaston toimesta ajan tasalle ennen kentälle viemistä, joten alussa pieni potkustartti päivitysjärjestelmään liitettäessä on vielä suhteellisen helppo suorittaa. Testauksen ja johtopäätösten tulisi olla valmiina kuuden viikon aikana.

3.4.7 Käyttöönotto

Olettaen testauksen sujuneen riittävän hyvin, päivitysjärjestelmä voidaan ottaa todelliseen käyttöön. Tämä toteutetaan viidessä vaiheessa: Ensin asennetaan palvelimen ohjelmistot uudelleen, sitten määritetään viralliset nimet päivitettävien koneiden ryhmille ja ryhmitellään ne lopulliseen muotoonsa, lisätään uusiin ryhmiin sen toimipisteen työasemat, missä testaus suoritettiin, seurataan tilannetta jonkin aikaa ja lopuksi palvelin viedään lopulliseen sijoituspaikkaansa sekä lisätään loput koneet sen alaisuuteen. Samalla laaditaan lyhyehkö, mutta kattava ohjeistus päivitysjärjestelmän käytöstä. Mikäli aiemmat vaiheet venyvät arvioitua pidemmiksi, voidaan harkita päivityspalvelimen uudelleenasennuksen sivuuttaminen ja asennettavien päivitysten määrittäminen sekä lataaminen uudelleen, jos mitään tarvetta tähän ei testauksen aikana ole havaittu.

3.4.8 Seuranta ja raportointi

Päivityspalvelimen tultua virallisesti käyttöön kaikki päivitykset kulkevat sen kautta ja siksipä ATK-osaston on valvottava palvelimen kuntoa ja muistettava hyväksyttää uudet päivitykset oikeisiin ryhmiin ajallaan. Alussa palvelimen toimintaa tulee vielä seurata muutaman kuukauden ajan tavallistakin tarkemmin, jotta mahdolliset yllätykset havaittaisiin ajoissa. Muistiinpanojen pohjalta laaditaan lopullinen raportti ja asennusohjeet. Tarkkailu hoidetaan kesäkuukausien aikana ja raportti viimeistellään valmiiksi syyslukukauden aikana.

3.5 Suunnitelman toteutus käytännössä

Tarkennettukin suunnitelma on kuitenkin vasta kehys, jonka puitteissa työn tulisi parhaassa tapauksessa edetä. Kaikkea ei kuitenkaan voida aina ennakoida ja joitakin työvaiheita ei siksi välttämättä voida suorittaa suunnitelman mukaisessa järjestyksessä. Seuraavaksi käydäänkin läpi varsinainen toteutusprosessi erilaisine käänteineen.

3.5.1 Toteutusvaihtoehdon valinta

Jo aivan alkuvalmistelujen alussa päivitysjärjestelmien joukosta ykkösehdokkaaksi nousi WSUS, sillä paitsi että sen voi asentaa ilmaiseksi Windows-palvelimille, on se myös ominaisuuksiltaan riittävän kattava täyttämään annetut vaatimukset. WSUS hoitaa oikeastaan vain juuri ne tehtävät, mitä päivitystenjakelupalvelimelta olimme vaatimassakin, minkä johdosta sen ohjeistus on suhteellisen helposti lähestyttävissä ja nopeasti omaksuttavissa. Vastaavasti SMS ja sen seuraajat ovat jo niin laajoja ominaisuuksiltaan, että pelkän päivitystenjakelujärjestelmän takia sen perusteita ei kannattaisi alkaa opettelemaan. Annetun aikataulun rajoissa tuskin ehtisi edes alustavasti suunnitella miten monen palvelimen voimin SMS oltaisiin ottamassa käyttöön ja miten se sulautettaisiin optimaalisesti yrityksen toimialueeseen. Vastaavasti WSUS-palvelimen asennusoppaasta pystyi nopeasti hahmottamaan mikä asennusvaihtoehto olisi sopivin ja mitkä puolestaan ovat sen laitteisto- ja ohjelmistovaatimukset.

3.5.2 Testiympäristö

Testausvaihe päätettiin suorittaa yrityksen Nurmijärvellä sijaitsevan toimipisteen suunnitteluosaston tiloissa, jotka tuolloin koostuivat projektin kannalta hiukan ahtaasta toimistohuoneesta ja samankokoisesta, mutta melko täyteen ahdatusta ATK-varastosta. Palvelimen saapumista odotellessa käytiin läpi varaston koneita, joista koottiin kaksi työasemaa testausta varten. Windows 2000-testausta varten tehtiin vanhasta IBM NetVista työasemasta ”Testi2k” ja vastaavasti Windows XP asennettiin ”TestiXP” nimellä vähän tuoreemmalle HP dx2200 työasemalle. Työskentelytilojen ahtaudesta johtuen enempää testikoneita ei pystytetty, vaan päätettiin ensin saada Testi2k ja TestiXP kommunikoimaan WSUS-palvelimen kanssa ja lisätä vasta sen jälkeen lisää muuttujia yhtälöön. Työasemat pinottiin neuvottelupöydälle ja räkkipalvelin sai aluksi sijaita työpöydän päädyssä jotta siihen päästäisiin nopeasti käsiksi tarvittaessa. Testivaiheen loppupuoliskolla palvelin siirrettiin ATK-varaston puolelle ja sen hallinta hoidettiin etänä.

Työskentelytilojen ja resurssien rajallisuudesta johtuen tuleva WSUS-palvelin liitettiin suoraan yrityksen toimialueeseen, sillä erillisen testiverkon pystyttäminen todettiin vaativan liikaa vaivaa, minkä lisäksi pahimmassa tapauksessa testiverkko olisi aiheuttanut ylimääräisiä tai peittänyt todellisia ongelmia palvelimen toiminnassa. Päätöstä helpotti etenkin se seikka, että WSUS ei juurikaan aiheuta verkolle kuormaa itsekseen, vaan se palvelee vain niitä koneita, jotka ovat erikseen määritetty sitä käyttämään.

3.5.3 WSUS-palvelimen tarvitsemien palvelujen ja ohjelmien asennus

Palvelimen saavuttua siihen ei tarvinnutkaan asentaa käyttöjärjestelmää, vaan siinä oli jo Windows Server 2003 R2 esiasennettuna. Palvelinta odotellessa WSUS-palvelimen asennusopas oli tullut tutuksi ja niinpä nyt päästiinkin aloittamaan asennuksen valmistelu saman tien. WSUS 3.0:n asennusta varten tulee Windows Server 2003 palvelimessa olla asennettuna IIS, .NET 2.0, Microsoft Management Console 3.0 ja Microsoft Report Viewer 2005. Näistä .NET ja MMC olivatkin jo palvelimessa valmiina, joten asensimme vain IIS-palvelun sekä MS:n raporttikatselimen. Vaikka työasemien päivityspyyntöjen ohjaus WSUS-palvelimelle ja päivittämiseen liittyvien asetusten määritys vaikutti järkevimmältä hoitaa aktiivihakemiston kautta, se jätettiin asentamatta testipalvelimelle, jottei olisi jouduttu miettimään miten se pitäisi tehdä, kun verkossa oli jo valmiina AD-palvelimia. Testipalvelimen aktiivihakemistoa ei olisi ollut järkevää mennä pintapuolisen tietämyksen nojalla yhdistämään olemassa olevaan hakemistoon ja sen eriyttäminen nosti esiin liikaa muita kysymyksiä. Käytimme lopulta olemassa olevaa aktiivihakemistoa, koska erillisten testausta varten luotujen organisaatioyksiköiden alle tehdyt ryhmäkäytännöt koettiin minimoivan riittävästi kaikki riskit. Palomuuriin on tarvittaessa määritettävä WSUS-palvelimelle käyttöön portit 80 ja 443, minkä lisäksi mahdollisen välityspalvelimen tulee tukea HTTP ja SSL protokollia.

3.5.4 WSUS-palvelimen asennus ja asetusten määrittely.

Kohdeyrityksen WSUS-palvelimen asennuksen ja siihen liitettyjen työasemien asetusten tarkan läpikäymisen sijasta asennus ja sen jälkeen määritetyt perusasetukset käsitellään seuraavaksi yleisellä tasolla käyden läpi eri vaihtoehtoja, joista joidenkin kohdalla voidaan tarkemmin perustella miten ne auttavat täyttämään kohdeyrityksen asettamat vaatimukset.
Asennusohjelma kysyy ensiksi halutaanko asentaa WSUS-palvelu vai pelkkä hallintakonsoli, jälkimmäinen mahdollistaa WSUS-palvelun hallinnan muiden koneiden kautta. Seuraavaksi tulee

päättää minne ladatut päivitykset tallennetaan ja sen jälkeen määritetään erillinen kohdekansio päivitysten tietokannalle, joka kannattaisi sijoittaa fyysisesti eri levylle, jotta palvelun suorituskyky paranisi. Lopuksi asennusohjelma pyytää määrittämään palvelulle verkkosivuston, jonka kautta WSUS osoittaa työasemat käyttämään itseään. Sivuston porttinumeroa ei voi asennuksen aikana vapaasti valita, mutta se voidaan käydä muuttamassa haluttuun muotoon asennuksen jälkeen.

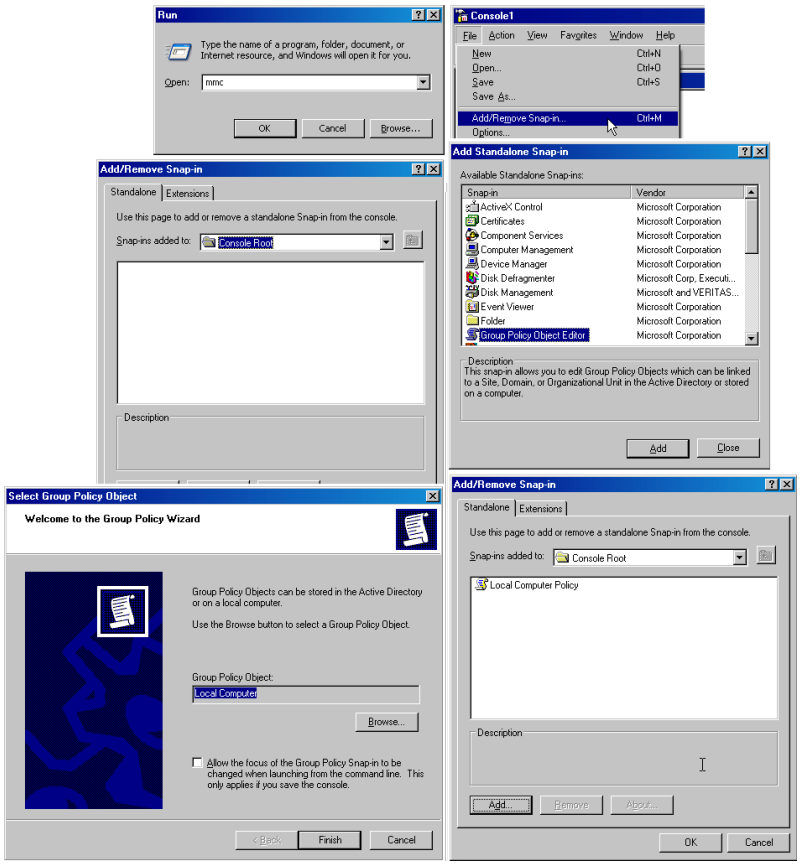
Asennuksen jälkeen käynnistyvän ohjatun toiminnon eli velhon avulla määritetään WSUS-palvelin käyttökuntoon. Ensin määritetään ns. yläjuoksun palvelin, jonka kautta WSUS ylläpitää saatavilla olevien päivitysten tietokantaansa ja tarvittaessa lataa hyväksytyt päivitykset. Ensimmäiselle WSUS-palvelimelle tulisi tietenkin valita Microsoftin päivityspalvelin, mutta jo kahden WSUS-palvelimen kanssa olisi hyvä laittaa toinen niistä alipalvelimeksi, joka saa tietonsa ensimmäisen kautta. Tällöin myös pitäisi määrittää kuinka itsenäisesti alajuoksun palvelin toimii, sen hallinta voidaan siis jättää joko paikallisen ylläpidon vastuulle tai sitten kaikesta päätetään verkon ylimmän WSUS-palvelimen kautta. Ketjutettaessa palvelimia on muistettava, että alipalvelin voidaan määrittää lataamaan päivitystietoja vain niistä päivityksistä jotka on valittu sitä ylemmällä tasollakin. Tämä siis tarkoittaa sitä, että ohjelmistojen ja käyttöjärjestelmien kaikki käytössä olevat kieletkin on lisättävä pääpalvelimen seurannassa oleviin päivityksiin, mikäli eri maassa olevien toimipisteiden työasemien päivitysten hyväksyntää ei haluta hajauttaa paikallistasolle. Toisaalta keskitetyllä hallinnalla voidaan alipalvelimilla jättää lataamatta vain tarpeettomat kieliversiot, kaikkien valittujen ohjelmistojen hyväksytyt päivitykset on pakko ladata vaikka alipalvelimen tarvitsisi jakaa päivityksiä vain esim. Windows XP -työasemille. Työasemia ei myöskään voida määrittää hakemaan käyttöjärjestelmän päivityksiä yhdestä palvelimesta ja vaikkapa jonkin MS Office -version päivityksiä toisesta, vaan ylläpidon pitäisi esim. ryhmäkäytännön kautta käydä vuoron perään muuttamassa päivityslähteen osoitetta.

Mahdollisen välityspalvelimen tiedot tulee antaa velholle ennen kuin se voi ottaa yhteyden aiemmin määritettyyn päivityslähteeseen. Yhteyden muodostuttua ladataan ylemmän tason palvelimelta tiedot kaikista päivitettävissä olevista ohjelmistoista ja eri päivitysluokista, joiden joukosta tehdään päivityspalvelimen alaisuuteen liitettävien työasemien tarpeita vastaavat valinnat. Valintojen jälkeen määritetään miten tiheästi palvelimen halutaan käyvän tarkistamassa isäntäpalvelimeltaan onko uusia päivityksiä, ohjelmistoja tai päivitysluokkia ilmaantunut saataville. Seuraavaksi velho tarjoutuu käynnistämään hallintakonsolin sekä synkronoimaan valittujen oh-

jelmistojen saatavilla olevien päivitysten tiedot päivityspalvelimelle. Lopuksi vielä listataan joitakin valinnaisia toimenpiteitä ja annetaan niille linkit tarkempiin ohjeisiin.

3.5.5 Työasemien ohjaus WSUS-palvelimelle

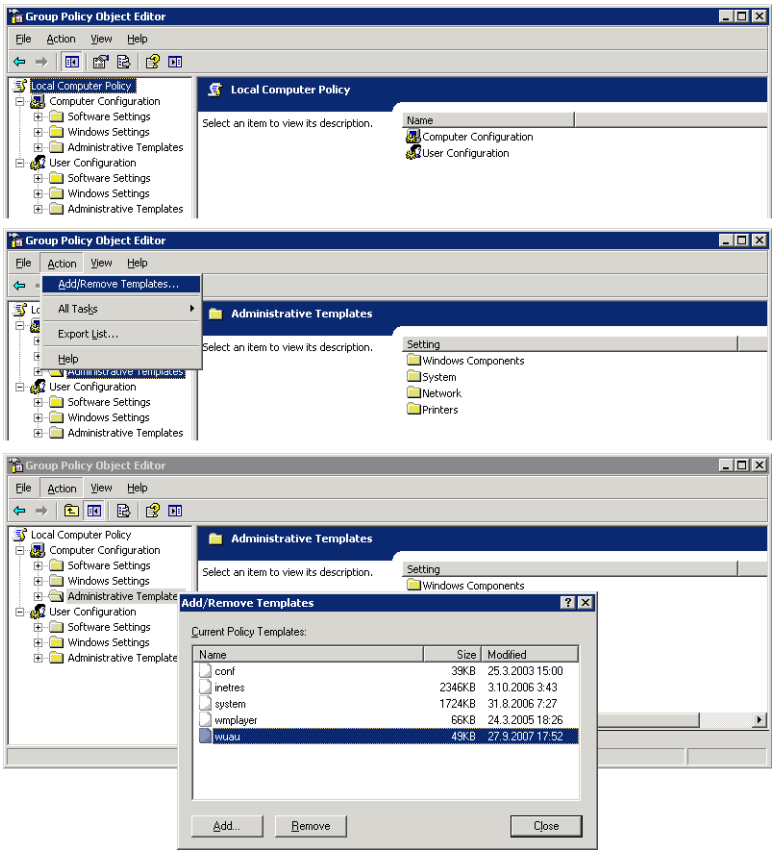
Jotta työasemat voidaan määrittää käyttämään WSUS-palvelinta päivityslähteenään, tulee niihin tai ryhmäkäytäntöjä hallinoivissa palvelimissa olla käytössä riittävän uusi versio wuau.adm -hallintapohjasta. Yrityksen AD-palvelimelle hallinnointipohjaa ei tarvinnut päivittää, mutta tarvittaessa tuorein wuau.adm saadaan esim. päivittämällä yksi Windows XP -työasema Windows Update -palvelun kautta, jonka jälkeen uusin hallintapohja löytyy Windowsin asennuskansion ”inf” -alikansiosta. Riippuen miten työasemat ohjataan päivityspalvelimelle, tulee uudempi hallintapohja ottaa käyttöön joko työasemilla tai palvelimilla paikallisten käytäntöjen kautta Group Policy Object Editor (GPOE) -ohjelman avulla.



Kuva 14: Paikallisten käytäntöjen avaaminen ryhmäkäytäntöeditorilla.

Paikalliset käytännöt ja GPOE eivät kuitenkaan ole suoraan käytettävissä, vaan ensin avataan Microsoft Management Console, lisätään editori ja valitaan sen kohteeksi paikallinen tietoko-

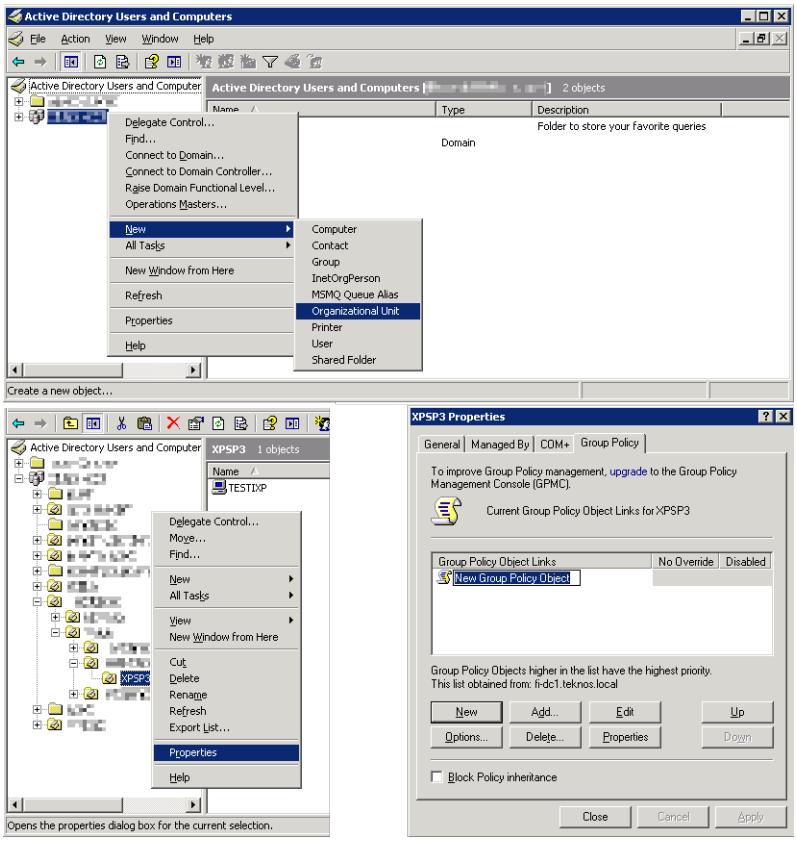
ne. Seuraavaksi valitaan Administrative Templates ja Action-valikosta Add/ Remove Templates, jonka avaamasta ikkunasta nähdään onko koneelle ladattu wuau.adm -tiedosto. Tarvittaessa se lisätään tai korvataan uudemmalla versiolla Add-painikkeen kautta.



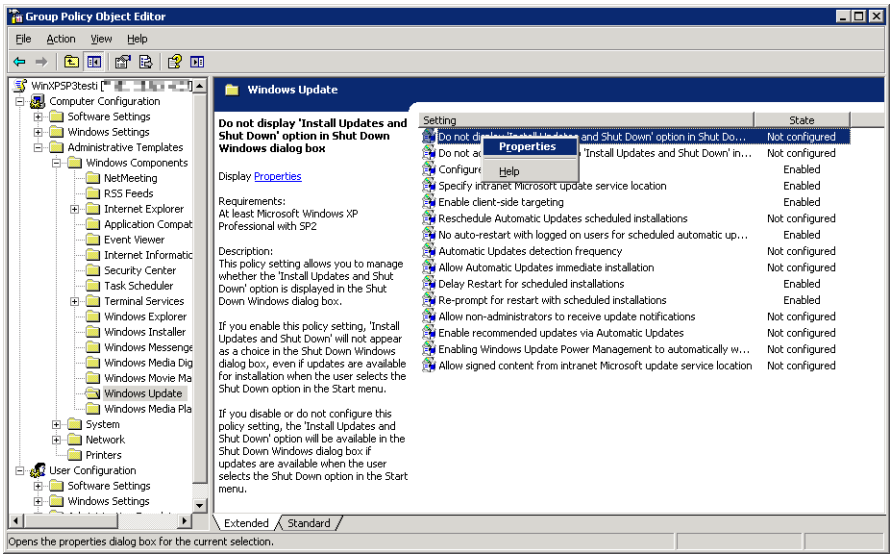
Kuva 15: WSUS:n Administrative Template:n lisäys/tarkistus.

WSUS-palvelin voidaan asettaa työasemien käyttämäksi päivityslähteeksi joko ryhmäkäytäntöjen tai paikallisten käytäntöjen avulla. Muutos onnistuu myös Windows-käyttöjärjestelmien rekisteriä muokkaamalla, mutta GPOE:n kautta ylläpidon ei tarvitse muistaa aivan kaikkea ulkoa, vaan kaikki asetusvaihtoehdot ovat nähtävissä ohjeistuksen kera. Koska ryhmäkäytännöt mahdollistavat vaivattomimman tavan hallita miten työasemat ryhmitellään sekä määrittää miten ja milloin niiden päivitysten tulisi asentua, esitellään päivitysasetusten muokkaus aktiivihakemiston kautta tehtynä. Aluksi luodaan uusi organisaatioyksikkö (Organization Unit, OU) testikoneita varten. Alempaan ”kansioon” luotuna se perii ylemmälle yksikölle luodut käytännöt, joten hyvin suunnitellulla hakemistorakenteella voidaan kaikki laajemmin käytössä olevat asetukset määrittää ylemmillä tasoilla ja alemmilla organisaatioyksiköillä lisätään käytäntöihin enää vain poikkeuksia. Uuden GPO:n luomiseksi avataan OU:n ominaisuudet ja valitaan Group Policy -välilehti, jonka kautta voidaan myös lisätä ennalta luotuja käytäntöjä sekä tehdä muutok-

sia. Muokkaus tehdään valitsemalla haluttu GPO ja painamalla Edit-painiketta, joka avaa valitun käytännön muokattavaksi GPOE:n avulla. Aiemmin käsitelty wuau.adm siis lisäsi hallintapohjiin päivityskäytäntöjä koskevat asetukset, jotka siis löytyvät polun "..\Computer Configuration\Administrative Templates\Windows Components\Windows Update" alta.



Kuva 16: Uuden OU:n ja GPO:n luonti.



Kuva 17: Päivityskäytäntöjen sijainti.

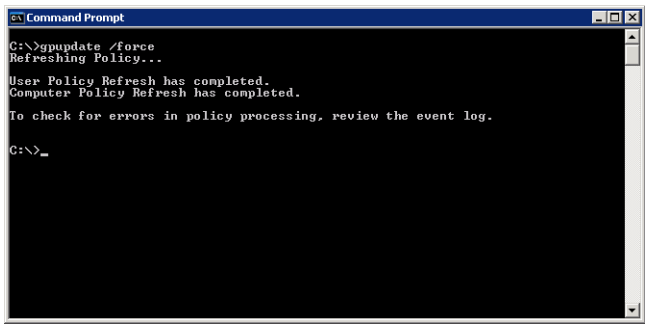
Kuvasta 17 nähtävillä asetuksilla määritetään päivityslähteen lisäksi monia muita päivittämiseen liittyviä toimintoja, joista osan voi määrittää muutakin kautta, mutta ryhmäkäytännön puolelta tehtynä ei paikallisella koneelle enää voida muuttaa niitä omin luvin. Kuvasta voidaan myös nähdä status- eli tilasarakkeessa osalla riveistä termi ”Not configured”. Tällöin asetus ei ole joko käytössä tai se peritään ylemmältä tasolta.

Jokaisesta asetuksesta annetaan seuraavaksi lyhyt kuvaus:

- Do not display 'Install Updates and Shut Down' option in...
  Sammutettaessa konetta ei käyttäjälle listata mahdollisuutta asentaa ensin päivityksiä.
- Do not adjust default option to 'Install Updates and...
  Sammutusta edeltävää päivityssessiota ei tarjota oletuksena, eikä siten kiireessä valita.
- Configure Automatic Update Properties
  Määrittää milloin ja miten päivitykset asennetaan tai estetään ne kokonaan.
- Specify intranet Microsoft update service location Properties
  Päivityslähteen osoitteen määritys, eli ohjaa työasemat esim. WSUS-palvelimelle.
- Enable client-side targeting Properties
  Työasemaryhmälle voidaan määrittää ryhmänimi, jonka alle WSUS sijoittaa.
- Reschedule Automatic Updates scheduled installation Properties
  Odotetaanko seuraavaa päivää vai päivitetäänkö aiemmin, jos edellinen kerta jäi välistä.
- No auto-restart with logged on users for scheduled automatic updates ins...
  Estetään automaattinen uudelleenkäynnistys päivitysten päätteeksi.
- Automatic Updates detection frequency Properties
  Saatavilla olevien päivitysten tarkastustiheyden määritys, tunneissa.
- Allow Automatic Updates immediate installation Properties
  Windowsin toimintaa häiritsemättömien päivitysten välittömän asennuksen sallinta.
- Delay Restart for scheduled installations Properties
  Määritetään viive ennen päivityksen jälkeistä uudelleenkäynnistystä.
- Re-prompt for restart with scheduled installations Properties
  Määritetään viive ennen uudelleenkäynnistyksestä muistutetaan toistamiseen.
- Allow non-administrators to receive update notifications Properties
  Sallii päivitysilmoitukset muillekin kuin vain järjestelmänvalvojille.

- Enable recommended updates via Automatic Updates Properties
  Sallii suositeltavien päivitysten asennuksen tärkeiden lisäksi.
- Enabling Windows Update Power Management to automatically wake up...
  Määrittää saako virranhallinta herättää koneen lepotilasta päivittymään.
- Allow signed content from intranet Microsoft updates service location Properties
  Mahdollistaa sertifioidut päivitykset muiltakin tahoilta kuin Microsoftilta.

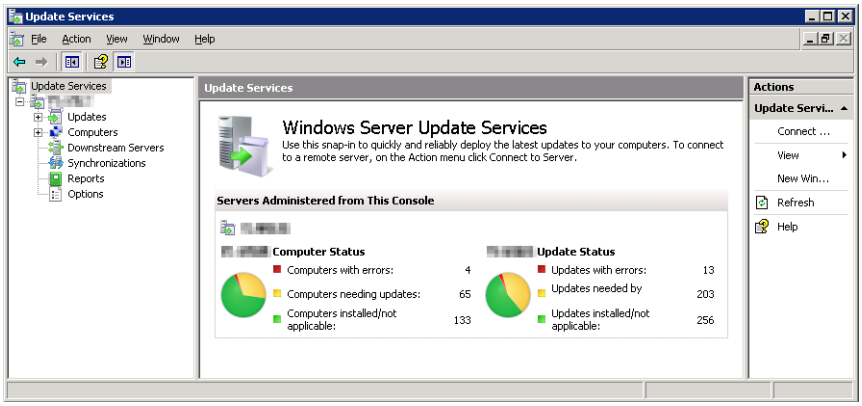
Client Side Targeting mahdollistaa työasemien kohdistamisen haluttuihin ryhmiin suoraan käytäntöjen puolelta, jolloin WSUS-palvelun hallintakonsolissa vain luodaan käytännössä nimetty ryhmä ja kaikki käytännön alaiset työasemat ohjautuvat siihen. Liitettäessä uusi työasema toimialueeseen se pitää vain siirtää sopivaan organisaatioyksikköön, eikä hallintakonsolissa tarvitse käydä lainkaan. Toisaalta määrittämällä WSUS toimimaan Server Side Targeting -tilassa, voidaan työasemia siirtää hallintakonsolin puolella ryhmästä toiseen tarpeen mukaan. Kummassakin vaihtoehdossa on omat etunsa ja niiden arvottaminen riippuu pitkälti siitä onko WSUS-palvelimen ylläpitäjällä myös pääsy aktiivihakemiston asetuksiin vai ei. Käytännön kautta voidaan määrittää samalla useampikin ryhmä, jolloin ne erotetaan toisistaan puolipilkuilla. Tälle voisi olla hyötyä esim. luomalla jokaiselle ohjelmistolle WSUS-palvelun hallintakonsolissa oma ryhmänsä johon hyväksytään vai kyseisen ohjelmiston päivitykset. Vastaavasti työasemat ryhmiteltäisiin niiden tarvisemien ohjelmistokokonaisuuksien mukaan.



Kuva 18: Muutosten välitön käyttöönotto.

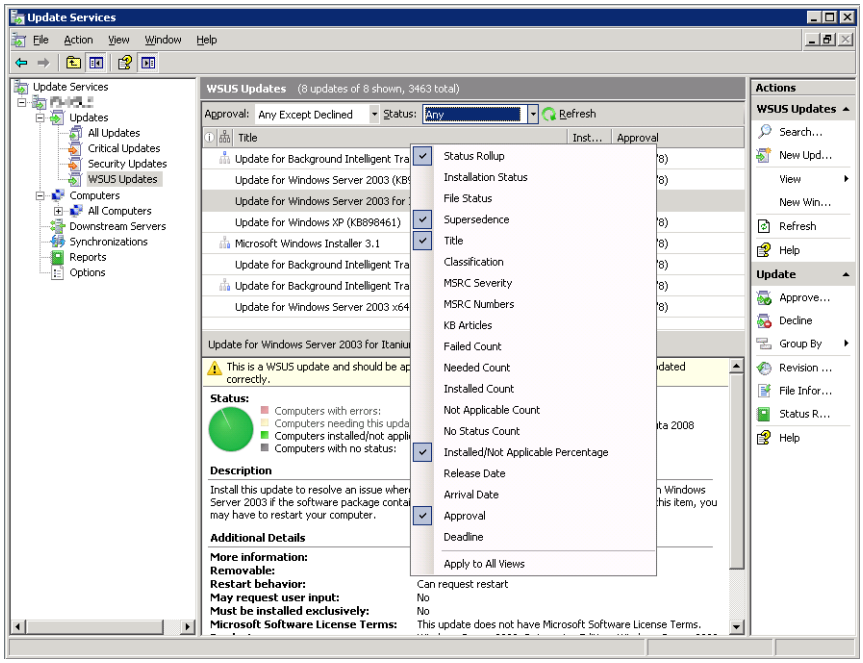
Muokatut käytännöt astuvat voimaan pienelle viiveellä, mutta ne voidaan pakottaa käyttöön välittömästi komentorivikomennolla ”gpupdate /force”. Ryhmäkäytännöiden kohdalla käsky pitää ajaa sekä hallintapalvelimella, että niillä tietokoneilla, joille muutos halutaan heti voimaan.

3.5.6 WSUS-palvelun hallintakonsoli



Kuva 19: WSUS, hallintakonsoli.

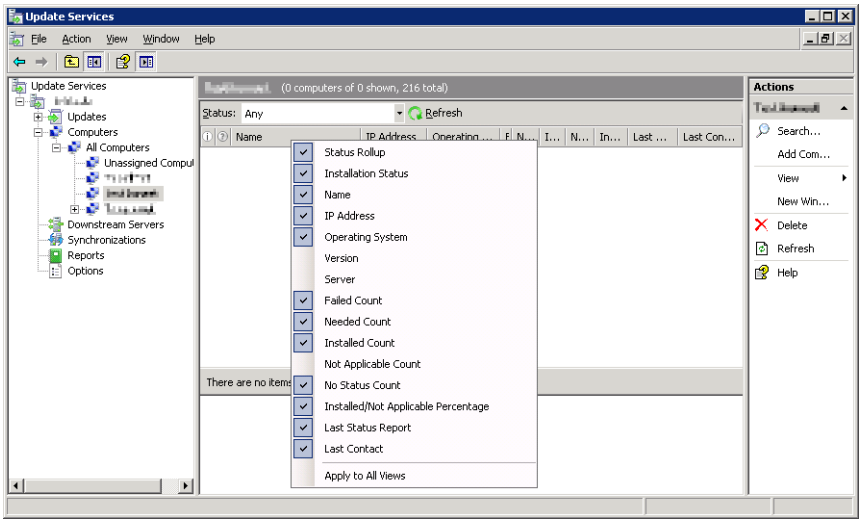
WSUS-palvelun ylläpitoa varten sille on palvelimella oma hallintakonsoli, joka voidaan asentaa myös työasemille, jotta palvelimeen ei tarvitse kirjautua paikallisesti eikä etänä. Mikäli samaa palvelinta hallintaan useammalta konsolilta, on muistettava etteivät päivitysvalikkoon luodut näkymät päivity muille konsoleille. Itse määritetyt näkymät eivät ole pakollisia, mutta niiden avulla rajataan saatavilla olevat päivitykset mielekkäämpiin ryhmiin. Juuritasolla nähdään montako WSUS-palvelinta konsoliin on liitetty ja lyhyt yhteenveto niissä asioivien työasemien päivitystilanteesta. Jokaisen palvelimen alta taas haarautuu näkyville valikkorivit päivityksille, tietokoneille, alajuoksun palvelimille, Synkronointien historialle, raporteille ja palvelimen asetuksille. Valitsemalla päivitykset tai tietokoneet saadaan yhteenveto niiden alla olevista päivitysnäkymistä tai koneryhmistä.



Kuva 20: Päivitysnäkymän sarakkeiden valinta.

Päivityshaaran valmiit näkymät listaavat kaikki kriittiset päivitykset yhdessä ja tietoturvapäivitykset toisessa ryppäässä, minkä lisäksi voidaan valita näkyville kaikki päivitykset tai vain WSUS-palvelua koskevat. Vähintäänkin jokaiselle käytössä olevalle Windows- ja Office-versioille kannattaisi luoda omat näkymänsä, jotta päivitysten läpikäynti olisi mielekkäämpää. Uutta näkymää luotaessa määrittään mitkä ohjelmistot ja päivitystyypit sen halutaan listaavan, listattavissa ovat tietenkin vain ne päivitykset, mitä WSUS-palvelimelle itselleen on rajattu seurattavaksi. Valitsemalla jokin näkymä saadaan kuvan 20 mukaisesti sen listaamat päivitykset ylempään osaan konsolia ja valitsemalla jokin päivitys saadaan sen tarkemmat tiedot näkyville listan alle. Päivityslistan sarakkeita voidaan lisätä tai poistaa klikkaamalla hiiren oikealla näppäimellä jotain saraketta. Molemmat Status- sekä Supersedence -sarakkeet kannattaa ottaa näkyville, sillä niistä saa nopeasti nähtyä mikä on päivitysten asennustarve, ja -tilanne sekä korvaako päivitys aiemman päivityksen vai onko se itse jäänyt vanhaksi. Valitettavasti korvattuja päivityksiä ei sovi mennä suoralta käsin merkitsemään kokonaan poistettavaksi, vaan ensin tulee varmistaa että myös korvaava päivitys on tarkoitettu samoille käyttöjärjestelmille kuin edeltäjänsä. Windows XP:n SP3 saattaa sisältää uudemman version jostain päivityksestä, mutta ei tuota korjauspakettia tietenkään saa Windows 2000:lle asennettua.

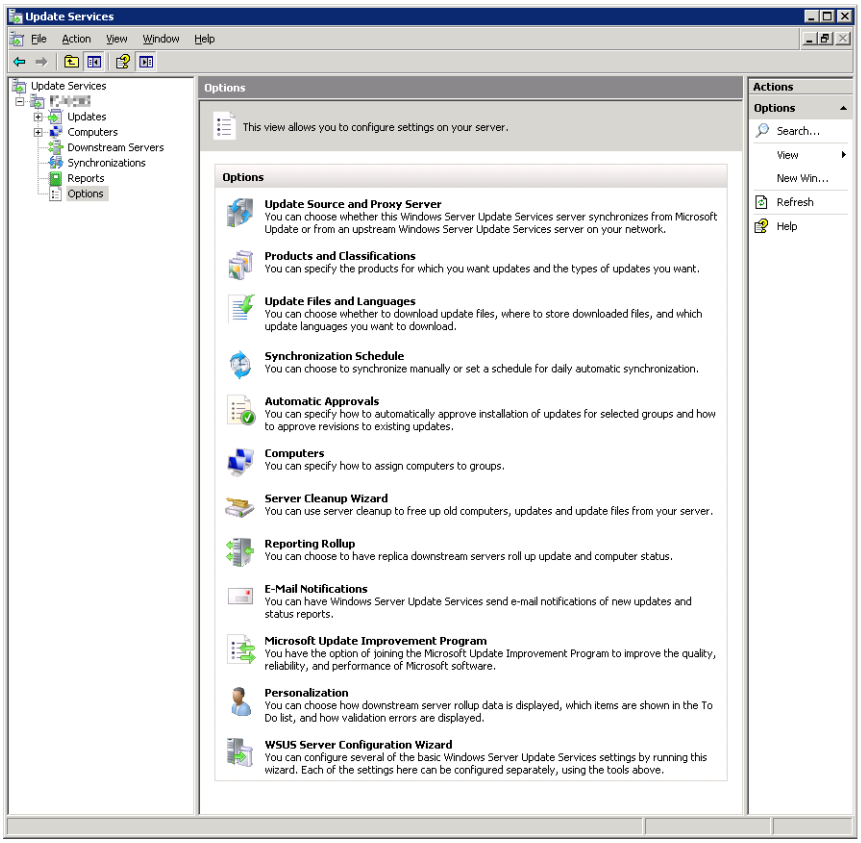
Oikea hiirinappi avaa valitun päivityksen kohdalla esiin valikon, jossa voidaan mm. saada siitä selville aiempien versioiden historia ja joko hyväksyä tai kieltää päivitys. Hyväksyntä avaa uuden ikkunan, jossa listataan tietokoneryhmään luodut kansiot. Valitsemalla jokin kansion voidaan oikeasta napista hyväksyä päivityksen asennus tai poisto sekä perua aiempi hyväksyntä. Tietokonehaarassa määritetyt työasemaryhmät on voitu luoda hakemistopuuksi, jolloin hyväksyttäessä päivitystä voidaan sille annettu tila periyttää valitun kansion lapsille tai vanhemmille, eli haaran alemmille tai ylemmille ryhmille. Kriittiset päivitykset näyttäisivät hyväksyttävän itsensä automaattisesti alemmille kansioille. Mikäli jokin päivitys pitäisi hyväksyä myös täysin erillisessä haarassa, olisi se hyvä tehdä samalla kertaa. Helpoin tapa löytää uudet päivitykset on listata vain hyväksymättömät, mutta mikäli ne hyväksyy yhteenkin tietokoneryhmään, ovat ne muidenkin päivitysnäkymien mukaan hyväksyttyjä. Tosin mikäli tästä tuntuisi muodostuvan suurikin ongelma, voi tietokonehaaran ryhmittelyssäkin olla jotain pahasti pielessä. ”Hukkuneet” päivitykset löytyvät viimeistään katsomalla tietokoneryhmän puolelta mitä päivityksiä koneet ilmoittavat tarvitsevansa, jolloin ne voidaan hyväksyä suoraan saadun raportin kautta.



Kuva 21: Tietokonehaaran sarakkeiden valinta.

Tietokonehaaran kaikki omat ryhmät luodaan All Computers -ryhmän alle. Luomalla jokaiselle päivitysnäkymälle vastaavan tietokoneryhmän ja määrittämällä ryhmäkäytännöissä työasemille useamman kohderyhmän niihin asennettujen ohjelmistojen mukaan ei päivitysten periytymisestä välttämättä tarvitse huolehtia lainkaan. Aktiivihakemiston puolella ei kuitenkaan ole järkeä luoda erilliset organisaatioyksiköt ja käytännöt jokaiselle käyttöjärjestelmän ja Office-versioiden yhdistelmälle, joten joko ohjelmistokantaa tulisi yhdenmukaistaa tai hyväksyttää kaikki käyttöjärjestelmät yhteen yhteen ryhmään ja toimisto-ohjelmistot toiseen. Jos jotain ohjelmis-

totyyppiä ei sitten saisi jollain koneella päivittää, niin sille luotaisiin oma OU, jossa tuon ohjelmiston ryhmää ei mainittaisi.



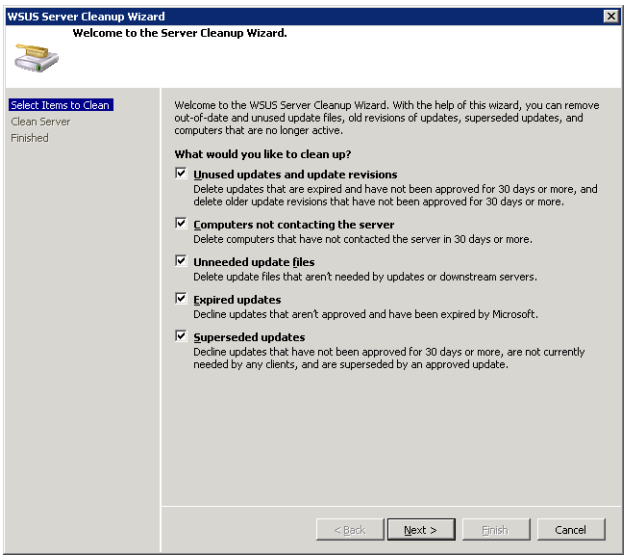
Kuva 22: WSUS-palvelimen omat asetukset.

Lopuissa haaroissa ei sitten enää ole juurikaan mitään sanottavaa, alipalvelimien tiedot ja WSUS-palvelimen oman päivityslähteen synkronointihistoria on aika yksiselitteistä ja raportteja voidaan luoda suoraan päivitys- ja tietokonehaaroistakin käsin. Jäljelle jää enää WSUS-palvelimen omien asetusten haara, jossa siinäkin osa valinnoista jo tehtiin asennuksen ja asetusvelhon aikana, joka voidaan ajaa nyt täältä käsin tarvittaessa uudelleen. Asetushaarassa on kuitenkin muutama tärkeä valinta, joita ei velhon aikana päästy määrittämään.

- Avaamalla Update Files and Languages voidaan päättää säilötäänkö päivityksiä lainkaan WSUS-palvelimella vai halutaanko ne jostain syystä yhä hakea joka koneelle erikseen. Samasta ikkunasta voidaan myös käskyttää WSUS lataamaan päivitykset Express Installation Files -muodossa, jolloin niiden jakelu kuormittaa vähemmän lähiverkkoa.
- Computers-rivin kautta päätetään hoidetaanko työasemien kohdistamien WSUS-ohjelmiston päivitysryhmiin hallintakonsolin vai ryhmäkäytäntöjen kautta. WSUS voidaan

myös laittaa sähköpostittamaan tilanneraportteja ylläpidolle, jotta päivityksiä ei unohdettaisi kaikessa kiireessä hyväksyä. Siihenkin hätään löytyy Automatic Approvals -toiminto, jolla voidaan luoda hyväksymissääntöjä samalla periaatteella kuin päivitysnäkymien rajauksiakin.

- Jotta palvelimen levytilaa ei haaskattaisi vanhentuneilla päivityksillä, voidaan asetuksista käynnistää Server Cleanup Wizard eli siivousvelho, jolla myös esim. käytöstä poistuneet työasemat saadaan poistettua.



Kuva 23: Siivousvelhon asetukset.

3.6 Testaus ja käyttöönotto

Edellä käytiin läpi ns. käytännöllisin tapa hoitaa sekä työasemien ryhmittely että niiden päivityskäytäntöjen määritys. Kuitenkaan testausvaiheen alkupuoliskolla ei vielä oltu aivan varmoja siitä pitäisikö aktiivihakemistoon koskea lainkaan, sillä vaikka AD oli käytettävissä, ei siihen vielä tuolloin ollut yrityksen sisällä oikeastaan kukaan ehtinyt syvällisemmin perehtymään. Niinpä ensin testattiin saataisiinko testikoneet ylipäätänsä päivittymään edes paikallisten käytäntöjen kautta ja samalla tutustuttiin hallintakonsolin käyttöön. Kun palvelimelle saatiin latautumaan ensimmäiset päivitykset niiden hyväksynnän jälkeen, voitiin alkaa selvittämään uskaltaisiko aktiivihakemistoa käsitellä ilman aikaisempaa kokemusta koko asiasta. Onneksi aktiivihakemisto osoittautui lopulta riittävän ymmärrettäväksi, jotta koimme kykenevämme hyödyntää sitä työasemien päivityskäytäntöjen hallintaan. Olisihan ollut jokseenkin hullunkurista, jos keskitetty päivitystenjakelujärjestelmämme olisi vaatinut kaikkien työasemien asetusten määrittämisen erikseen jokaisen muutoksen yhteydessä. Organisaatioyksiköillä ja ryhmäkäytännöillä saimme aikaan meille sopivan hakemistorakenteen, jossa eri tyyppisiä päivityksiä ja niiden asennukseen liittyviä asetuksia varten ei tarvittu luoda liian montaa OU:ta.
Alunperin testaamiselle piti olla alkuvalmistelujen jälkeen käytettävissä koko huhti- sekä toukokuu, mutta palvelimen toimitus kangerteli sen verran pahasti, että se saapuikin vasta huhtikuun puolessa välissä. Aikataulua ei haluttu venyttää, joten tilanteeseen sopeuduttiin miettimällä miten testausta voitaisiin laajentaa mielekkäästi minimoimalla samalla mahdolliset riskit. Päädyimme lopulta lisäämään toimihenkilöiden työasemat päivitystestien piiriin toukokuun alussa. Tuotannon työasemiin ei vielä koskettu, sillä niitä käytetään myös ilta- ja yövuorossa, jolloin päivityksiin liittyvien ongelmien ratkominen olisi täytynyt jättää aamulle. Lisäksi virheestä ei välttämättä olisi saatu edes riittävän selkeää kuvausta, jolloin vikaa olisi pitänyt etsiä sokkona tai jäädä odottamaan koska ilmoittajan vuoro taas alkaa.

Ennen oikeassa käytössä olevien koneiden lisäämistä testipalvelimen alaisuuteen ainoat ongelmat olivat johtuneet vain siitä, että testikoneissa ei ollut kaikkia WSUS-palvelimen kanssa kommunikointiin tarvittavia päivityksiä valmiiksi asennettuina. Ilman joitakin komponentteja esim. Windows 2000 ei olisi voinut kommunikoida palvelimen kanssa lainkaan ja myös jotkin toiminnot olisi WSUS-palvelun pitänyt osata päivittää suoraan tai ainakin tarjota työasemille ladattavaksi ns. Client Self Update -toiminnon avulla. Tätä ei kuitenkaan saatu toimimaan tai ainakaan palvelun asennusopasta seuraamalla jokin tuntui olevan pielessä. Tarkemmin asiaa tutkittaessa selvisi, että Windows 2000 tarvitsi vähintään kolmannen ja Windows XP ensimmäi-

sen korjauspaketin asennuksen, jotta automaattiset päivitykset -toiminto olisi riittävän uusi pelatakseen yhteen WSUS-palvelun kanssa. Ilman riittävän tuoretta korjauspakettia pitäisi koneille voida asennettava SUS Client Installer, mutta sitäpä ei enää näytä Microsoftin sivulta löytyvän, vaikka sille yhä linkkiä saman firman Technet-sivustolla tarjotaan. Eli mikäli olisi todella hyvä syy jättää korjauspaketit asentamatta, ei WSUS-palvelimen käyttökään todennäköisesti tule onnistumaan. Onneksi kohdeyrityksen konekanta voitiin ja oli päivitetty riittävän pitkälle, jotta ne toimisivat WSUS-palvelun kanssa ilman SUS Client Installer -paketin etsimistä epämääräisemmiltä verkkosivuilta. Mikäli jokin vanhempi ATK-varastossa lojuva työasema vielä vaatisi uudelleenasennuksen, olisi järkevintä asentaa siihen suoraan tuorein korjauspaketti jo ennen virustorjunnankaan asennusta ja lähiverkkoon kytkemistä.

Toukokuun aikana WSUS-palvelin oli jo periaatteessa täydessä käytössä samassa toimipisteessä kuin missä sen testauskin suoritettiin. Ja koska testivaiheen aikana oli todettu WSUS-palvelimen täyttävän sille asetetut vaatimukset, sen käytöstä laadittiin kuun lopussa alustava ohjeistus ja kesäkuun alussa palvelin pakattiin pääkonttoriin kuljetusta varten. Pääkonttoriin saavuttaessa palvelin sijoitettiin paikalleen ja sen kolmesta verkkoportista kaksi linkitettiin vikasietoisuuden lisäämiseksi. Operaatio ei kuitenkaan sujunut aivan ongelmattomasti, sillä palvelimelle jouduttiin asentamaan sen valmistajalta sivuilta ladattu päivitys ennen kuin linkitys saatiin toimimaan. Hallintakonsolin käyttö puitiin pikaisesti läpi, minkä jälkeen sen hoitovastuu oli nyt periaatteessa ylläpidon käsissä. Palvelimen toiminnan seuraus ja laajemman raportin kirjoittamien kuitenkin jatkui tämän jälkeen.

3.7 Seuranta ja tulokset

Testivaiheen aikana ei todellista käyttöä voitu täysin simuloida, eikä siihen olisi aikakaan kunnolla riittänyt, kun keskityimme ajamaan päivityksiä testikoneisiin uudelleen ja uudelleen mietien samalla miten työasemat ryhmiteltäisiin ja niiden asetukset määriteltäisiin. Lisäksi testikoneet ja ylläpidon omat työasemat tavattiin käynnistää uudelleen heti kuin vain mahdollista, joten kaikki muutokset olivat aina astuneet täysin voimaan ennen kuin töitä jatkettiin. Tavalliset käyttäjät kuitenkin kiireessä helposti siirtävät uudelleenkäynnistyspyynnöt sivuun, jolloin jokin päivitetty ominaisuus ei välttämättä toimi ennen kuin seuraavana työpäivänä, kun työasema käynnistetään uudelleen. Kaiken lisäksi toimihenkilöiden koneet oli määritetty päivittymään taustalla, joten mikäli jokin päivitys ei suoralta käsin vaatinut uudelleenkäynnistystä, ei käyttäjä välttämättä edes huomannut päivitysten ajoa. Ideaalisissa olosuhteissahan tässä ei pitäisi olla mitään ongelmia, mutta saimme kesän mittaan kuulla, että joissain työasemissa ei enää Internet Explorer -selain toiminutkaan. Vika ei kuitenkaan tuntunut vaivaavan kaikkia käyttäjiä eikä iskenyt koneisiin samanaikaisesti, minkä lisäksi se korjautui joko pelkällä uudelleenkäynnistyksellä tai ajamalla koneelle ensin vielä sille asentamatta olevat päivitykset. Lopulta syyksi todettiin IE6-selaimen päivitys IE7-versioon, sillä jostain syystä operaatio ei asentanut kaikkea tarvitsemaansa kerralla eikä edes vaatinut uudelleenkäynnistystä välissä, joten selain saattoi olla jumissa seuraavan työpäivän päivitysajoon saakka. Hajanaiset ilmoitukset siis johtuivatkin siitä, etteivät kaikki olleet tarvinneet nettiä päivitysten välissä, minkä lisäksi esim. käyttäjien lomien ja saldovapaitten aikana koneet eivät suljettuina ollessaan tietenkään voineet päivittyä samaan aikaan muiden työasemien kanssa. Myöhemmin samantyyppinen ongelma esiintyi myös IE8-selaimeen siirryttäessä, mutta tälläkään kertaa se ei aiheuttanut mitään suurempia toimenpiteitä, vaan valtaosa työasemista ehti päivittyä kunnolla loppuun asti ennen kuin kukaan huomasi käyttää selainta.

Microsoftin .NET -kirjastojen päivittämisessä havaittiin myös omat ongelmansa, sillä esim. version 3.0 kielipaketin asennus näyttäisi epäonnistuvan mikäli työasemassa on jo asennettuna .NET 3.5. Työasema yrittää kuitenkin asentaa päivityksen joka päiviä uudelleen ja virheen korjaamiseksi pitäisi joko päivitys hylätä tai poistaa koneelta ylläpidon toimesta .NET-versiot 3.5, 3.0 ja varmuuden vuoksi vielä 2.0, minkä jälkeen asennetaan 3.0:n tuorein versio koneelle ja varmistetaan, että kielipaketti asentuu ennen 3.5-versiota. Tämä on kuitenkin aikaa vievä operaatio ja nostaa esiin kysymyksen miksi eri versioita ei joko ole sulautettu yhteen tai eriytetty täysin irti toisistaan, jotta päivitysten asennusjärjestys ei voisi aiheuttaa ongelmia.

Asennusjärjestyksen kanssa on havaittu ongelmia myös Windows XP SP3:n ja IE-selaimien eri versioiden kanssa. WSUS tarjoaa työasemille ensin selaimen eri versioiden päivityksiä, mutta ainakin version 8 kohdalla asennus epäonnistui, koska sen vaatima toinen päivitys oli aiemmin hallintakonsolissa todettu vanhentuneeksi, joten se poistettiin jakelusta. Tietysti ensin oli varmistettu, ettei sitä mikään kone enää kaivannut ja että korvaava päivitys oli jo hyväksytty sekä se myös todella oli tarkoitettu samalle käyttöjärjestelmälle. Oletus kuitenkin oli, että tuorein korjauspaketti asennetaan ylipäätänsä aina ensimmäisenä tai että WSUS ainakin tarjoaisi sen selainpäivitysten rinnalla. Ongelma tosin havaittiin vain, koska asensimme erääseen koneeseen käyttöjärjestelmän uudelleen valmistajan levyiltä ja siten koneesta puuttui tuo sekä tuo poistettu päivitys että myös SP3. Kuten jo aiemmin tuli todettua, kannattaisi vasta-asennettuihin työasemiin asentaa tuorein SP käsin ennen verkkoon liittämistä.

Päivitysten asennuksen epäonnistuessa työasemalle jää merkintä ”Windows Update.log” -tiedostoon, mutta virheelle annettu koodi ei välttämättä auta löytämään todellista syytä vikaan. Esimerkiksi IE8-selaimen asennuksen tarvitseman päivityksen puuttuminen selvisi lataamalla erillinen IE8-asennustiedosto, joka sitten kertoi ajettaessa mitä koneeseen pitäisi ensin asentaa. Linux-järjestelmien paketinhallintaa tuskin tullaan ihan heti Windows-puolella näkemään, mutta Microsoftin omien ohjelmistojen keskinäiset riippuvuudet voisi sentään edes kuvitella olevan hallittavissa WSUS-palvelun kaltaisen ratkaisun avulla. Eli hyväksyttäessä tai poistaessa jotain päivitystä jostain ryhmästä WSUS osaisi kertoa mitä muuta tarvitaan tai voidaan lisätä/poistaa samalla.

4 Yhteenveto

Työn tavoitteena oli ratkaista päivittämisen automatisointi menettämättä kuitenkaan hallintaa päivitysten ennalta hyväksyntään ja sallimatta kaikille koneille yhteyttä lähiverkon ulkopuolelle. Järjestelmän tuli myös antaa riittävästi tietoa työasemien päivitystarpeesta, sillä esim. joillekin käyttäjäryhmille haluttiin antaa vapaus valita itselleen sopiva hetki päivitysten asentamiselle, joten ylläpidon täytyisi pystyä seuraamaan ettei tuo hetki lykkääntyisi loputtomiin voidakseen tarvittaessa ystävällisesti muistuttaa asiasta.

Vaatimusten lisäksi työn rajoittavina tekijöinä toimivat käytettävissä oleva aika ja muut resurssit, esim. testausvaiheelle olisi saanut hyvän varaslähdön, mikäli oppilaitokselta olisi tarjottu Microsoft Dreamspark tai MSDN Academic Alliance -pohjaista opiskelijalisenssiä Windows Server 2003:lle jo kolme vuotta sitten eikä vasta viime joulukuussa. Oma WSUS-palvelin kotiverkossa olisi ollut hyvä lähtökohta alkuvalmisteluille ja se olisi toiminut hyvänä apuna palvelimen asennusta käsittelevillä kursseillakin, joissa käsitellyt asiat olisi voinut kotona toistamalla jopa oppia muistamaan. Myös ryhmäkäytäntöjen muokkaus palvelimella jonka häiriöt voisivat jopa seisauttaa tuotannon olisi voitu minimoida mikäli tarvittavat asetukset olisi voitu ensin opetella kotipalvelimen puolella. Toisaalta nyt vältyttiin miettimästä olisiko ollut opiskelijalisenssin vastaista tehdä palkalliseen työhön liittyviä testejä kotipalvelimella.

WSUS-palvelimen pystytys täytti kohdeyrityksen asettamat vaatimukset ja maksuttomana ohjelmistona sille voidaan lisätä tarvittaessa alipalvelimia jopa ilman merkittäviä lisäkustannuksia mikäli toisista palvelimista löytyy tarpeeksi resursseja ajamaan WSUS-ohjelmistoa muiden palveluidensa rinnalla. Vastaavasti ilmaisuuden hintana WSUS-palvelun kautta voidaan päivittää vain Microsoftin ohjelmistoja, tosin puutteen voi nähtävästi kiertää, jos on valmis ostamaan sopivan ohjelmiston, jolla pitäisi voida pakata muiden valmistajien ohjelmat WSUS-palvelun ymmärtämään muotoon. Pitkän seurantavaiheen aikanakaan ei tätä kuitenkaan testattu, sillä laman johdosta kaikki hankinnat olivat jäissä ja niinpä tuotteelle ei ostolupaa kuitenkaan olisi saatu. Ehkäpä hiljalleen olisi kuitenkin aika harkita asiaa uudelleen, sillä vaikka WSUS ratkaisee jo suurimman ongelman päivittämällä ns. pakolliset ohjelmistot eli Windows-käyttöjärjestelmät ja MS Office -toimistosovellukset, ei olisi pahitteeksi saada myös ne vähemmän laajasti käytössä olevat ohjelmistot jaettua saman palvelun kautta.

Vaikka tarpeet saattaisivat sittenkin vaatia SMS-tyyppisen järjestelmän hankintaa, on WSUS kohtuullisen yksinkertainen järjestelmä oppia käyttämään ja sen saa melko nopeasti otettua käyttöön, joten sitä voi käyttää väliaskeleena ylläpidolle suunnitellessa monimutkaisemman järjestelmän toteutusta.

Testivaiheessa olisi voitu kokeilla virtualisointia ja siten luoda huomattavasti enemmän testikoneita, joille olisi myös asennettu laajempi ohjelmistokirjo luomaan vaihtelua ja ehkä paljastamaan pienemmällä otannalla piiloon jääviä ongelmia. Muistiinpanoja olisi myös kannattanut tehdä ennakoivasti, eli kirjoittaa ensin mitä olisi tarkoitus tehdä ja jälkikäteen täsmentää mitä yllätyksiä tuli eteen. Merkinnät olisivat voineet olla monisanaisempiakin, sillä myöhemmin niitä lukiessa ei kaikki aikoinaan itsestään selvät vaiheet enää olleetkaan niin tuoreessa muistissa.

WSUS-palvelimen toimintaa on tultu seurattua nyt jo parin vuoden ajan ja voidaan sanoa sen toimineen kaiken kaikkiaan erinomaisesti, suurempia ongelmia ei ole havaittu. Aina silloin tällöin jokin kone tosin oikuttelee jonkin päivityksen asennuksen kanssa, mutta nyt se myös nähdään palvelimen raporteista ja asialle päästään heti miettimään selitystä, kun automaattisilla päivityksillä koneilta olisi pitänyt tarkistaa erikseen ovatko kaikki päivitykset asentuneet.

Alustavan ohjeistuksen jälkeen laajemman raportin teko jäi vapaa-ajalla tehtäväksi ja alunperin suunnitelmissa oli hoitaa se pois alta syksyllä, kun lukujärjestyksessä oli enää iltakursseja jäljellä. Kesän lopulla työsuhteesta tulikin vakinainen, joten kirjoitusaika hupeni johonkin töiden, kurssien, ja unen välimaille. Töiden johdosta ei unestakaan oikein voinut tinkiä, joten raportin kirjoittaminen pysyi jäissä ja viittä vaille unohduksissa kunnes kaikki kurssit oli saatu suoritettua ja oppilaitoksenkin ohjeistus tullut luettua uudelleen läpi. Tai olisi luettu läpi, jos sitä enää olisi saanut selkeässä omaa koulutusohjelmaa ja yksikköä koskevassa muodossa. Kaikkien tarvittavien välivaiheiden erottaminen vanhentuneista tai toista linjaa saati yksikköä koskevista ohjeista kesti oman aikansa ja aina jokin yksityiskohta alkoi hämäämään juuri kun kaiken piti olla selvää.

Kaikesta kuitenkin oppii, joten ensikerralla raporttia laadittaneen mahdollisimman valmiiksi käytännön toimien rinnalla ja sille on määritetty selkeä tavoiteaika.

Lähteet

Binner, S. SMS Package Construction. Luettavissa: http://www.winbatch.com/whitepapers/sms_package_construction.html. Luettu: 7.4.2010.

diTii.com 2007. Microsoft Update Catalog v1 Live. Luettavissa: http://www.ditii.com/2007/08/18/microsoft-update-catalog-v1-live. Luettu 31.1.2010.

Fisher, D. 2007. Microsoft should scrap Patch Tuesday. SearchSecurity. Luettavissa: http://searchsecurity.techtarget.co.uk. Luettu 26.1.2010.

HelpWithWindows.com 2005. Microsoft Update Site Launched. Luettavissa: http://www.helpwithwindows.com/microsoft-update.html. Luettu 21.2.2010.

Järvinen, P. 2006. Paranna tietoturvaasi. 1. painos. Docendo. Porvoo.

Kaiken maailman keksinnöt 1994. 1993. Tietokoneohjelmat. Alkuteos LE LIVRA MONDIAL DES INVENTIONS 1993. Gummerrus. Jyväskylä.

Keizer, G. 2006. Microsoft Keeps Software Update Services Alive Until July. Information-Week.com. Luetavissa: http://www.informationweek.com/news/security/showArticle.jhtml?articleID=194400595. Luettu 26.1.2010.

Keränen, V. 2005. Helpot ohjeet. Kotiverkosta turvallinen. Mikrobitti 1/2005. s. 63.

Kivimäki, J. 2005a. Windows Server 2003 – Tehokas Hallinta. 1. painos. Gummerus. Jyväskylä.

Kivimäki, J. 2005b. Active Directory – Tehokas Hallinta. 1. painos. Gummerus. Jyväskylä.

Klemencic, J. 2003. SUS Reporting Tool Luettavissa: http://home.fnal.gov/~jklemenc/susreport.html. Luettu: 24.3.2010.

Kytöhonka, A. 1989. Pieni tietokonesanasto. Koukkunen, K., Lehtinen, L., Mäki-Kuutti, T:, Saloranta, P. & Virtanen, T. Uusi Pikku Jättiläinen. 7. painos. WSOY. Porvoo.

McFedries, P. 1999. The complete idiot's guide to Windows 98. Luettavissa: http://books.google.com. Luettu 28.1.2010.

Microsoft. 2003. Systems Management Server 2003 Concepts, Planning, and Deployment Guide. Luettavissa: www.microsoft.com. Luettu: 6.4.2010.

Microsoft. 2005. Deploying Microsoft Windows Update Services. Luettavissa: www.microsoft.com. Luettu: 1.3.2008.

Microsoft. 2007. How to install multiple Windows updates or hotfixes with only one reboot. Luettavissa: http://support.microsoft.com/?kbid=296861. Luettu 17.3.2010.

Microsoft. 2008. Deploying Microsoft Windows Update Services 3.0 SP1. Luettavissa: www.microsoft.com. Luettu:1.4.2009.

Microsoft Technet 2010. Microsoft Security Bulletin Advance Notification. Luettavissa: http://www.microsoft.com/technet/security/bulletin/advance.mspx. Luettu 26.1.2010.

myITforum.com. 2009. The History of SMS. Luettavissa: http://www.myitforum.com/myITWiki/Default.aspx?Page=SMSHistory. Luettu 6.4.2010.

Mäntylahti, O. 1995. Konehuone. Kytke ja käytä. Pelit 4/1996. s. 14.

Naraine, R. 2004. Microsft Scraps Plans for Windows 2000 SP5. eWeek.com. Luettavissa: http://www.eweek.com/c/a/Windows/Microsoft-Scraps-Plans-for-Windows-2000-SP5. Luettu 21.2.2010.

Ohio Land Title Association. 2007. Title Topics – February 2007, Tech Talk. Luettavissa: http://www.olta.org/files/Feb07TitleTopics.pdf. Luettu 28.1.2010.

Office Sustained Engineering, 2009. Office 2000 and Office Update Site to Retire. Luettavissa: http://blogs.technet.com/office_sustained_engineering/archive/2009/05/20/office-2000-and-office-update-site-to-retire.aspx. Luettu 29.1.2010.

Oulun yliopisto 2006. Tietohallinto, tietoturvasivut. Windows-työaseman turvaaminen. Luettavissa:
http://www.oulu.fi/tietohallinto/tietoturva/sisalto/yllapito/windows/win-user/index.html. Luettu: 23.9.2009.

Savill, J. 2005. Q: What's the Microsoft Systems Management Server (SMS) OS Deployment Feature Pack? Windows IT Pro. Luettavissa:
http://www.windowsitpro.com/article/administration-tools2/q-what-s-the-microsoft-systems-management-server-sms-os-deployment-feature-pack-.aspx. Luettu: 7.4.2010.

Stasiukonis, S. 2006. Social Engineering, the USB way. Darkreading.com. Luettavissa:
http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634. Luettu: 15.4.2010.