HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Upravljanje sigurnosnim zakrpama korištenjem Software Update Services alata

CCERT-PUBDOC-2004-09-88

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. UVOD 4

2. PATCH MANAGAMENT 5

3. SOFTWARE UPDATE SERVICES 6

3.1. OPĆENITO 6
3.2. ARHITEKTURA 6
3.3. INSTALACIJA 7
3.3.1. SUS poslužitelj 8
3.3.2. Automatic Updates klijentska aplikacija 8
3.4. KONFIGURACIJA 9
3.4.1. Podešavanje poslužitelja 9
3.4.2. Podešavanje klijenta 14

4. ZAKLJUČAK 18

5. REFERENCE 18

1. Uvod

Redovito pregledavanje i pravovremena instalacija sigurnosnih zakrpi jedan je od temeljnih uvjeta za uspostavu sigurnog i pouzdanog informacijskog sustava. Sve veći broj sigurnosnih propusta unutar različitih programskih paketa i operacijskih sustava predstavlja ozbiljnu prijetnju za sigurnost informacijskih sustava ukoliko se ne poduzmu odgovarajuće preventivne mjere koje će omogućiti zaštitu potencijalno ranjivih sustava.

Problem redovitog praćenja sigurnosnih upozorenja (eng. *advisories*) i instalacije pripadajućih sigurnosnih zakrpi (engl. *patch*) posebno je istaknut u većim i heterogenim računalnim okruženjima gdje je potrebno voditi računa o velikom broju klijentskih i poslužiteljskih računala s različitim operacijskim sustavima i servisima. U takvim situacijama vrlo je teško na svim računalima održavati visoku razinu sigurnosti pogotovo ukoliko se u obzir uzme činjenica da je sve sigurnosne zakrpe prije primjene na produkcijska računala preporučljivo testirati kako bi se osigurala njihova "ispravnost" tj. kompatibilnost s postojećim aplikacijama.

Jedno od rješenja koje mrežnim administratorima olakšava proces pregledavanja računala te instalacije odgovarajućih zakrpi su tzv. *patch management* alati, kojima je osnovni cilj automatizirati i olakšati postupak upravljanja sigurnosnim zakrpama. Upravljanje sigurnosnim zakrpama ili *patch management* relativno je novo je područje računalne sigurnosti koje uključuje sve postupke i procedure vezane uz instalaciju sigurnosnih zakrpi.

U ovom dokumentu biti će opisan Software Update Services servis, jedno od Microsoftovih rješenja koje korisnicima omogućuje upravljanje postupkom instalacije sigurnosnih zakrpi. U nastavku dokumenta će biti opisani postupci instalacije i konfiguracije Software Update Service servisa, njegove prednosti i nedostatci, te mogućnosti primjene u praksi.

2. Patch managament

Iako proces instalacije sigurnosnih zakrpi na prvi pogled djeluje prilično jednostavno i logično, praksa i iskustvo pokazuju da postoje brojni problemi i ograničenja koji otežavaju provođenje ovih zadataka. Kao najbolji pokazatelj može se uzeti svakodnevna pojava novih sigurnosnih incidenata koji su najčešće posljedica iskorištavanja poznatih sigurnosnih problema za koje zakrpe nisu pravovremeno instalirane.

Dobro je poznato da su zakrpe za sigurnosne propuste koje su iskorištavali poznati maliciozni programi kao što su npr. Blaster, Slammer i sl., bile objavljene mnogo prije nego što su se pojavili sami maliciozni programi koji su ih iskorištavali. Obzirom da su navedeni programi prouzročili velike štete i financijske gubitke širom Interneta, opravdano je smatrati da se velik dio ovih gubitaka mogao spriječiti pravovremenom instalacijom odgovarajućih sigurnosnih zakrpi. Upravo se iz tog razloga u posljednje vrijeme počelo mnogo više pažnje posvećivati cjelovitim rješenjima koja bi omogućila bolju kontrolu i upravljanje nad postupkom instalacije sigurnosnih zakrpi.

Upravljanje sigurnosnim zakrpama moguće je implementirati nekom od sljedećih metoda:

- pojedinačnom instalacijom sigurnosnih zakrpi nakon što su javno objavljenje,
- korištenjem specijaliziranih programa ugrađenih u sam operacijski sustav ili programski paket,
- korištenjem specijaliziranih aplikacija nezavisnih proizvođača.

Koji će se od navedenih pristupa koristiti ovisi o specifičnosti okruženja u kojem se sustav koristi, potrebama i raspoloživom budžetu korisnika te o brojnim drugim faktorima.

U nastavku dokumenta biti će opisano korištenje Software Update Services programskog paketa, besplatnog rješenja koje Microsoft nudi svojim korisnicima.

3. Software Update Services

3.1. Općenito

Software Update Services (SUS) jedno je od Microsoftovih rješenja namijenjeno distribuciji i upravljanju sigurnosnim zakrpama u manjim i srednjim informacijskim okruženjima. Program je razvijen prema uzoru na popularni Windows Update servis koji korisnicima omogućuje automatsku instalaciju i održavanje kritičnih sigurnosnih zakrpi na Windows 2000/XP/2003 operacijskim sustavima, a posebno je efikasan ukoliko se primjenjuje u okruženjima s instaliranim Active Directory servisom (iako to nije neophodno). SUS servis instalira se u obliku Web aplikacije kroz koju je moguće upravljati sustavom te cijelim postupkom dobavljanja i instalacije sigurnosnih zakrpi.
Uspostavom SUS servisa implementira se lokalni Windows Update poslužitelj koji omogućava jednostavniju i bržu distribuciju sigurnosnih zakrpi na lokalnoj računalnoj mreži na kojoj je sustav postavljen.
Treba napomenuti da SUS servis omogućuje instalaciju sigurnosnih zakrpi samo za sljedeće proizvode/operacijske sustave:

- Windows 2000 s instaliranom SP2 sigurnosnom zakrpom,
- Windows XP,
- Windows 2003.

Tipovi sigurnosnih zakrpi koje se mogu instalirati su sljedeći:

- Windows Critical Updates
- Windows Security Patches (Critical, Important, Moderate, and Low)
- Windows Update Rollups
- Windows 2000, Windows XP, and Windows Server 2003 Service Packs

Zakrpama za Microsoft SQL, Exchange, Office i slične druge proizvode nije moguće primjenjivati ovim putem, što se može navesti kao jedan od nedostataka SUS servisa. Slično vrijedi i za ostale tipove zakrpi koje nisu navedene (zakrpe za upravljačke programe i sl.). Za cjelovita rješenja koja će omogućiti potpunu kontrolu nad postupkom instalacije svih sigurnosnih zakrpi i eventualno drugih programskih paketa potrebno je koristiti Microsort System Management Server programski paket ili neko od nezavisnih komercijalnih rješenja koja je moguće pronaći na tržištu.
Također, kao još jedan nedostatak SUS servisa treba navesti nemogućnost selektiranog dobavljana sigurnosnih zakrpi s Windows Update poslužitelja. To znači da korisnici čiji su sustavi bazirani isključivo na Windows 2000 operacijskim sustavima ne mogu dobaviti samo zakrpe za navedenu platformu, već moraju dobaviti sve zakrpe koje su trenutno raspoložive na Windows Update poslužiteljima. U sljedećim inačicama predviđeno je dodavanje ove funkcionalnosti, čime će se korisnicima omogućiti preciznija kontrola i odabir zakrpi primjenjivih u njihovom okruženju.

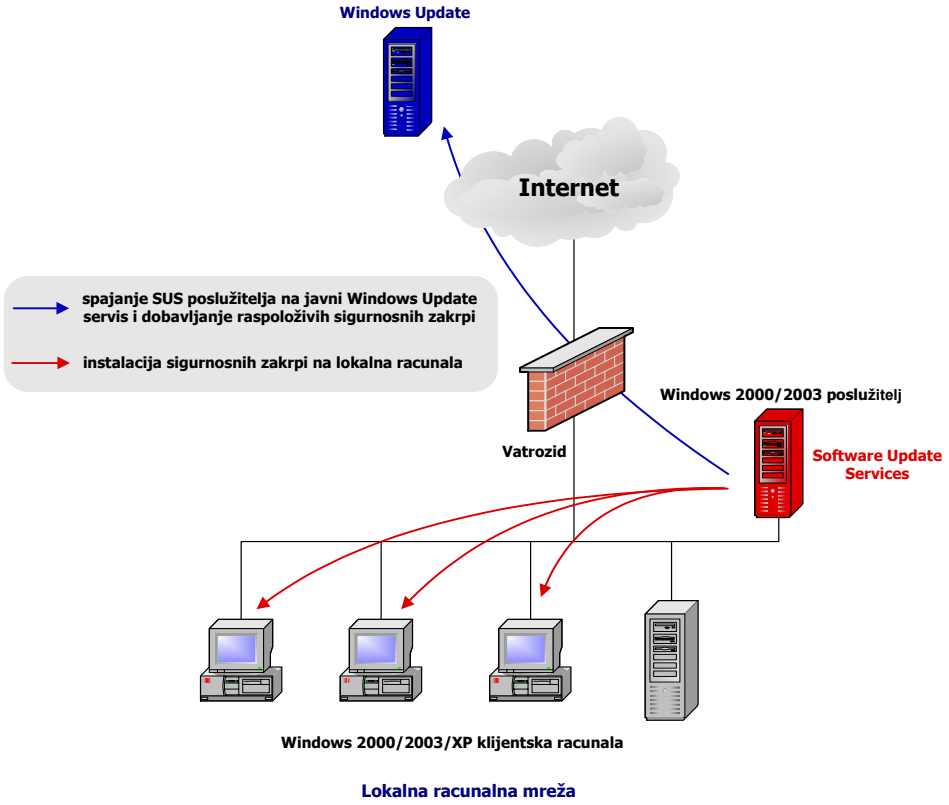
3.2. Arhitektura

Software Update Service servis sastoji se od dva dijela:

- Windows 2000/2003 poslužitelj s instaliranim **Software Update Services** servisom. Centralni SUS poslužitelj postavlja se na lokalnoj računalnoj mreži korisnika (iza vatrozida ukoliko isti postoji) te se u predefiniranim intervalima spaja na javne Windows poslužitelje u svrhu dobavljanja najnovijih sigurnosnih zakrpi. Sinkronizacija sa može provoditi ili automatski korištenjem ugrađenog *scheduler-a* ili ručno pritiskom na odgovarajuću karticu.
- Klijentska računala s instaliranim **Automatic Updates** servisom. Automatic Update servis uključen je u Windows 2000 operacijske sustave sa instaliranom SP3 sigurnosnom zakrpom (nadalje), Windows XP sustave sa SP1 sigurnosnom zakrpom (nadalje) te Windows 2003 operacijske sustave. Za Windows 2000/XP sustave bez navedenih sigurnosnih zakrpi istu je funkcionalnost moguće instalirati korištenjem odgovarajućeg programskog paketa.

Ovakva konfiguracija može se shvatiti kao dodavanje novog sloja u tradicionalni koncept instalacije zakrpi korištenjem javnog Windows Update servisa, budući da se na razini lokalne računalne mreže kreira lokalni Update poslužitelj kojeg će klijenti koristiti u postupku instalacije zakrpi. Lokalni SUS

poslužitelj periodički se spaja na javne Windows Update poslužitelje s kojih se dobavljaju nove sigurnosne zakrpe raspoložive za instalaciju. Ovisno o veličini i strukturi lokalne računalne mreže te broju klijentskih računala moguće je uspostaviti više SUS poslužitelja kako bi se podigle performanse sustava. Slika 1 prikazuje osnovni koncept korištenja Windows Software Update servisa.



Slika 1: Arhitektura Windows Software Update servisa

Neke od osnovnih prednosti korištenja SUS servisa:

- smanjenje troškova budući da se sve zakrpe samo jednom dohvaćaju s Interneta (ušteda *bandwidtha*),
- mogućnost testiranja zakrpi prije nego što se klijentskim računalima stave na raspolaganje,
- mogućnost odobravanja i blokiranja pojedinih zakrpi,
- centralizirani nadzor sustava upravljanja sigurnosnih zakrpi,
- jednostavno i intuitivno sučelje za upravljanje sustavom,

Na kraju svakako treba napomenuti činjenicu da je SUS programski paket potpuno besplatan, što korisnicima Windows 200/XP/2003 operacijskih sustava omogućuje jednostavnije održavanje visoke razine sigurnosti na svojim računalima bez direktnih financijskih troškova i ulaganja. Naravno, Windows operacijski sustav na kojem se pokreće SUS servis potrebno je licencirati, kao i sva klijentska računala koja ga koriste.

3.3. Instalacija

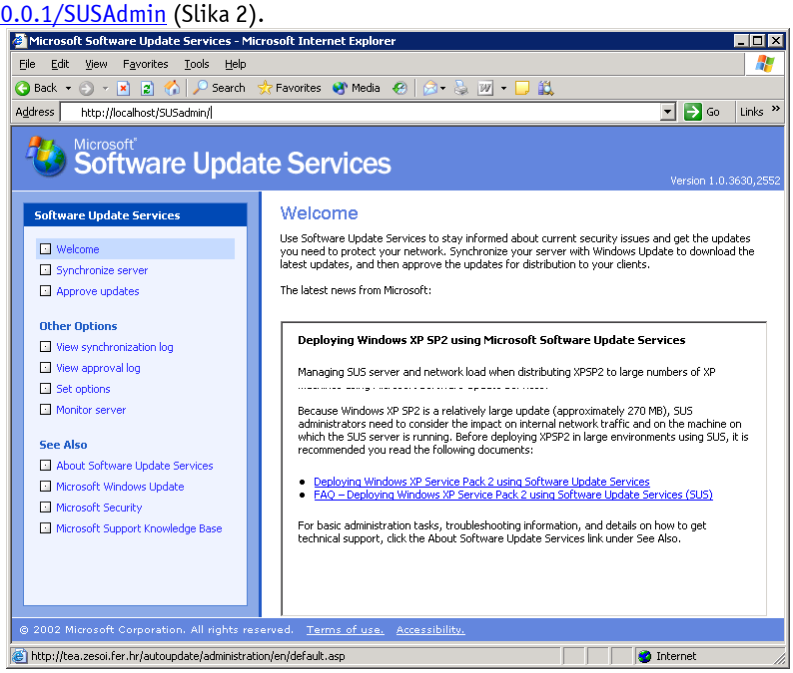
Kako je već ranije spomenuto SUS servis sastoji se od dva dijela: SUS poslužitelja, kroz koji se vrši upravljanje i distribucija sigurnosnih zakrpi te Automatic Updates klijentske aplikacije kojom se klijentska računala povezuju sa SUS poslužiteljem. U nastavku dokumenta bit će ukratko opisani postupci instalacije obje komponente SUS servisa.

3.3.1. SUS poslužitelj

Software Update Services programski paket moguće je instalirati na Windows 2000 Server operacijskim sustavima s instaliranom SP2 sigurnosnom zakrpom i novijim te na Windows Server 2003 sustavima. Na istom računalu potrebno je instalirati i IIS Web poslužitelj (inačica 5.0 ili novija) u okviru kojeg će se pokretati Web aplikacija za upravljanje sustavom. Za pristup sučelju potrebno je koristiti minimalno Internet Explorer 5.5 programski paket.
Prema preporukama proizvođača minimalni zahtjevi na hardverske resurse računala na kojem se pokreće SUS servis su sljedeći:

- Pentium III, 700 MHz CPU
- 512 MB radne memorije
- 6 GB slobodnog diskovnog prostora za instalaciju i pohranu sigurnosnih zakrpi.

Nakon što su zadovoljeni gore navedeni elementi moguće je krenuti sa postupkom instalacije sustava. Microsoft Software Update Services (SUS) 1.0 with Service Pack 1 (SP1) programski paket moguće je dohvatiti sa sljedeće URL adrese: http://www.microsoft.com/downloads/details.aspx?FamilyId=A7AA96E4-6E41-4F54-972C-AE66A4E4BF6C&displaylang=en. Instalaciju programa moguće je inicirati pokretanjem SUS10SP1.exe instalacijske datoteke, nakon čega će uslijediti postupak instalacije tipičan za Windows operacijske sustave. Nakon nekoliko dijaloških okvira unutar kojih je potrebno definirati osnovne parametre programa kao što su mjesto instalacije i sl. postupak instalacije je dovršen te je moguće pristupiti sučelju SUS servisa na sljedećoj adresi http://127.0.0.1/SUSAdmin (Slika 2).



Slika 2: *Glavno sučelje SUS servisa*

Ukoliko se program instalira na Windows 2000 Server operacijski sustav zajedno sa SUS servisom instalira se i IISLockdown alat čime se dodatno podiže sigurnost IIS Web poslužitelja.

3.3.2. Automatic Updates klijentska aplikacija

Kako bi se omogućilo dobavljanje i instalacija sigurnosnih zakrpi putem SUS servisa, na klijentska računala potrebno je instalirati odgovarajuću Automatic Updates aplikaciju. Spomenuta aplikacija dostupna je za Windows 2000/XP/2003 operacijske sustave, a instalacijsku datoteku moguće je dohvatiti s adrese:
http://www.microsoft.com/Windows2000/downloads/recommended/susclient/download.asp.

Spomenutu aplikaciju potrebno je instalirati na Windows 2000 operacijske sustave sa SP2 sigurnosnom zakrpom i Windows XP sustave bez sigurnosnih zakrpi, obzirom da zakrpe SP3 (za Win2k) i SP1 (za WinXP) u sebi uključuju spomenutu aplikaciju.
Postupak instalacije vrlo je jednostavan i sastoji se od pokretanja odgovarajuće instalacijske datoteke (WUAU22.msi). Nakon dovršene instalacije, postavke servisa moguće je uređivati ili lokalno korištenjem Automatic Updates sučelja unutar Control Panel-a (kod Windows XP sustava spomenuto je sučelje integrirano unutar System sučelja), ili na razini Windows domene korištenjem Group Policy objekta unutar Active Directory servisa. Detaljnije informacije o načinu podešavanja Automatic Updates servisa biti će dane u nastavku dokumenta (Poglavlje 3.4.2).
Instalacijom Automatic Updates servisa također se u *system tray* traci sustava pojavljuje ikona u obliku kugle s logotipom Microsoft Windowsa putem kojeg se korisnici koji su članovi lokalne *Administrators* grupe obavještavaju o novim sigurnosnim zakrpama raspoloživim za instalaciju (ukoliko je omogućena ova funkcionalnost). Ostali korisnici sustava neće biti obaviješteni o raspoloživim zakrpama.

3.4. Konfiguracija

Slično kao i kod postupka instalacije i postupak konfiguracije SUS servisa potrebno je obaviti i na poslužiteljskoj i na klijentskoj strani. U nastavku dokumenta bit će ukratko opisani postupci konfiguracije SUS poslužitelja i Automatic Updates klijenta koje je potrebno obaviti kako bi se omogućilo uspješno funkcioniranje sustava.

3.4.1. Podešavanje poslužitelja

Postupak konfiguracije i korištenja SUS servisa sastoji se od nekoliko faza koje će ukratko biti opisane u nastavku dokumenata. Radi se o sljedećim fazama:

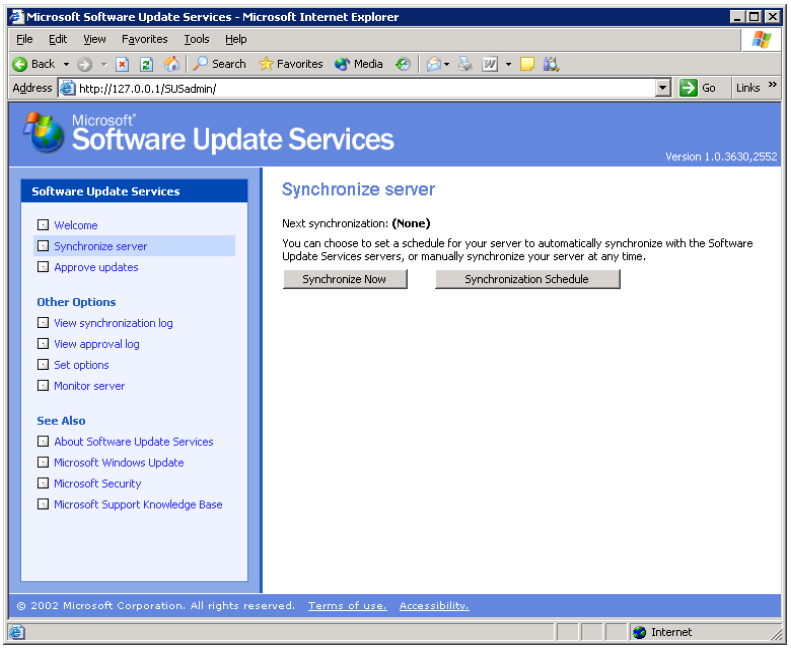
- sinkronizacija poslužitelja,
- odobravanje sigurnosnih zakrpi,
- praćenje i nadzor sustava.

3.4.1.1. Sinkronizacija poslužitelja

Kako bi se omogućila distribucija sigurnosnih zakrpi na lokalnoj računalnoj mreži, lokalni SUS poslužitelj potrebno je prvo sinkronizirati s javnim Windows Update poslužiteljima kako bi se dohvatile nove raspoložive sigurnosne zakrpe. Dva su osnovna tipa sadržaja koji se sinkroniziraju između lokalnog i javnih Windows Update poslužitelja:

- **Meta-data podaci** - podaci koji sadrže informacije o raspoloživim sigurnosnim zakrpama i pravilima njihove primjene. Meta-data podaci uvijek se dohvaćaju u procesu sinkronizacije kako bi se usporedilo stanje na lokalnom i udaljenom poslužitelju.
- **Update data** – podaci koji se instaliraju na sustav nakon što je odgovarajuća zakrpa odobrena za instalaciju.

Sučelje kroz koje je moguće obaviti sinkronizaciju poslužitelja prikazano je na sljedećoj slici (Slika 3), a moguće ga je odabrati pritiskom na vezu **Synchronize Server** unutar lijevog okvira glavnog prozora.

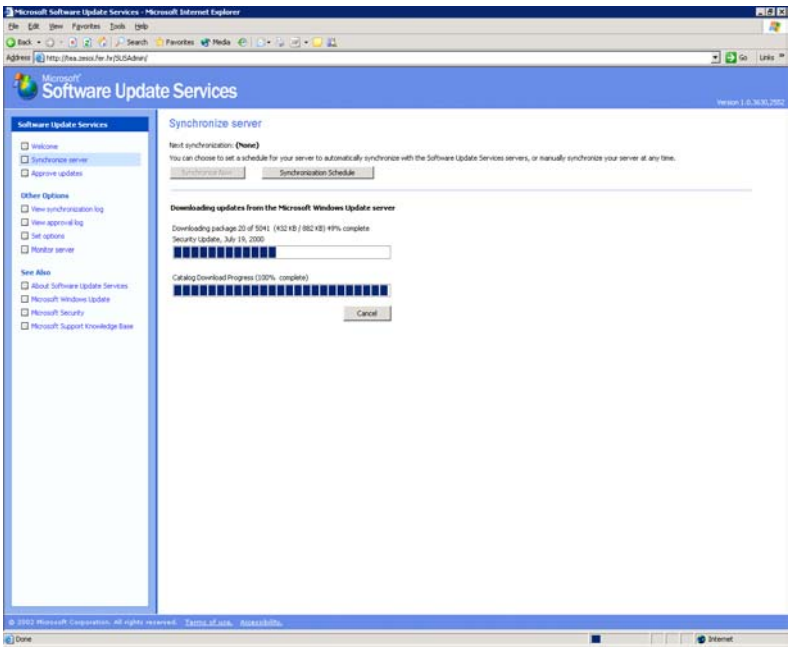


Slika 3: Sučelje za sinkronizaciju poslužitelja

Na slici se može uočiti da je sinkronizaciju poslužitelja moguće obaviti na dva načina: ručno, pritiskom na karticu **Synchronize Now** ili u predefiniranim vremenskim intervalima koje je moguće podesiti unutar **Synchronization Schedule** sučelja. Kako bi se osigurala pravovremena raspoloživost odgovarajućih sigurnosnih zakrpi preporučuje se korištenje kombinacije oba pristupa. Za osvježavanje na dnevnoj ili tjednoj bazi preporuča se korištenje ugrađenog *scheduler* programa, dok se ručno osvježavanje poslužitelja preporuča prilikom izlaska novih sigurnosnih zakrpi.

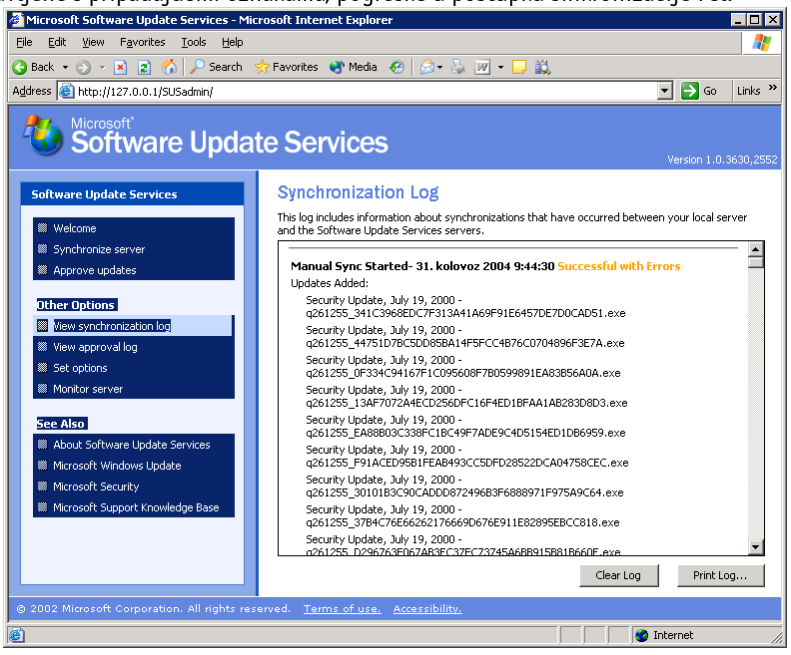
Proces sinkronizacije sastoji od nekoliko koraka: povezivanja s javnim Microsoft Windows Update poslužiteljima, dobavljanja najnovije inačice paketa s meta-data podacima o raspoloživim sigurnosnim zakrpama, provjere integriteta i autentičnosti dobavljenog paketa analizom pripadajućeg digitalnog certifikata te dobavljanja onih datoteka koje su izmijenjene od trenutka posljednje sinkronizacije. Osim dohvaćanja novih, osvježenih datoteka, proces sinkronizacije također uključuje i uklanjanje datoteka koje su iz određenog razloga povučene s javnih poslužitelja, čime je ostvareno da stanje lokalnog poslužitelja u svakom trenutku odgovara stanju na javnim Windows Update poslužiteljima .

Proces sinkronizacije, odnosno dohvaćanja novih i osvježenih datoteka s javnih Windows Update poslužitelja prikazan je na sljedećoj slici (Slika 4).



Slika 4: Proces sinkronizacije lokalnog SUS poslužitelja

Svi podaci o obavljenom postupku sinkronizacije bilježe se u log datoteku koju je moguće pregledati pritiskom na vezu **Synchronization Log** unutar okvira s lijeve strane (Slika 5). Generirani log zapisi sadrže bitne podatke o procesu sinkronizacije kao što su vremena početka i završetka, lista svih zakrpi koje su dobavljene s pripadajućim oznakama, pogreške u postupku sinkronizacije i sl.



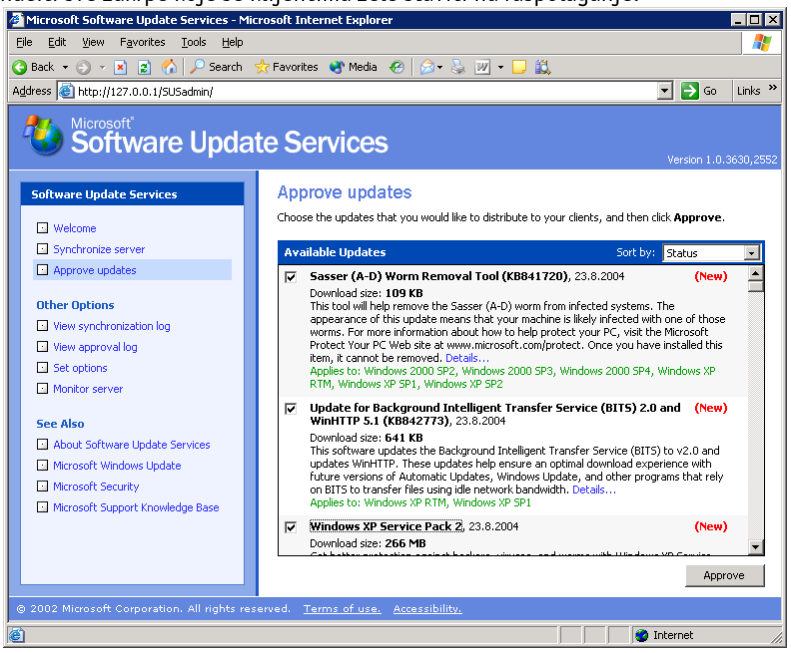
Slika 5: Log podaci o obavljenom postupku sinkronizacije

Nakon što je obavljena sinkronizacija lokalnog SUS poslužitelja, sigurnosne zakrpe raspoložive su za distribuciju na klijentska računala. No, kako bi se dohvaćene zakrpe stavile na raspolaganje klijentskim računalima, iste prethodno moraju biti odobrene od strane administratora sustava. Taj postupak će biti detaljnije opisan u nastavku poglavlja.

Postupak odobravanja sigurnosnih zakrpi iznimno je važan u cijelom procesu upravljanja sigurnosnim zakrpama, budući da administratorima omogućuje testiranje i provjeru kompatibilnosti svih zakrpi prije njihove instalacije na klijentska računala. Na taj način minimizira se rizik od eventualnog neželjenog utjecaja novo instaliranih zakrpi na raspoloživost informacijskog sustava i kontinuitet poslovnih procesa koji se baziraju na informatičkoj podršci.

3.4.1.2. Odobravanje zakrpi

Kao što je već spomenuto sve zakrpe dohvaćene na lokalni SUS poslužitelj, prije nego što se stave na raspolaganje klijentima, moraju prethodno biti odobrene od strane administratora. Odobravanje sigurnosnih zakrpi provodi se unutar **Approve Updates** sučelja (Slika 6), unutar kojeg je eksplicitno potrebno označiti sve zakrpe koje se klijentima žele staviti na raspolaganje.



Slika 6: Sučelje za odobravanje sigurnosnih zakrpi

Unutar prikazanog sučelja prikazane su sve sigurnosne zakrpe koje su u procesu sinkronizacije dohvaćene s javnih Windows Update poslužitelja, zajedno sa svim informacijama vezanim uz pojedinu zakrpu. Radi se o sljedećim podacima:

- imenu zakrpe (npr. Windows XP Service Pack 2),
- datumu izdavanja zakrpe,
- veličini paketa,
- statusu zakrpe (Currently Approved, Not Approved, Updated, New),
- kratkom opisu,
- vezi na stranicu s dodatnim informacijama o odabranoj zakrpi,
- informaciji o tome da li zakrpa zahtjeva ponovno pokretanje računala (eng. *reboot*),
- informaciji o ovisnosti o drugim zakrpama (eng. *dependencies*),
- listi platformi za koje je zakrpa primjenjiva.

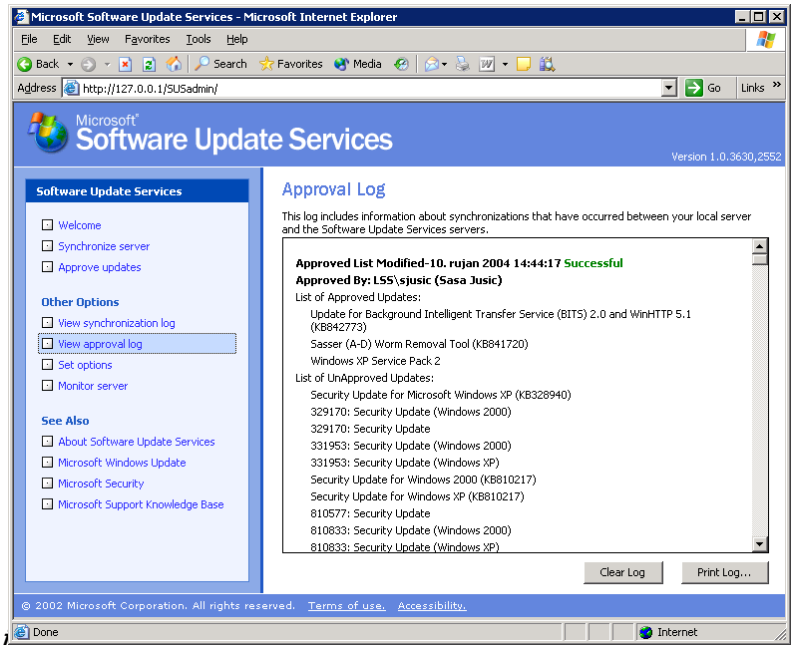
Listu zakrpi ujedno je moguće sortirati prema različitim kriterijima kako bi se olakšalo njihovo pregledavanje i pretraživanje. Kriteriji prema kojima je moguć prikaz zakrpi su datum, status, ime zakrpe i platforma za koju je ista primjenjiva.

Veza na detaljnije podatke o zakrpi (*Details*) sadrži sljedeće podatke o zakrpi:

- naziv i put do datoteke na tvrdom disku kojom je implementirana odgovarajuća zakrpa,
- listu parametara koje je potrebno proslijediti instalacijskom programu zakrpe ukoliko se ista pokreće putem naredbenog retka; korištenjem ovih parametara administrator sustava može pojedinu zakrpu instalirati neovisno od Automatic Updates servisa,

- listu jezika na kojima je zakrpa dostupna.
- vezu na lokalnu "**Read This First**" datoteku s detaljnijim podacima o zakrpi.

Postupak odobravanja zakrpi sastoji se od označavanja odgovarajućeg *checkbox* polja pokraj zakrpe koja se želi odobriti, te pritiska na gumb **Approve** na dnu stranice. Na sličan način moguće je i povući zakrpu sa liste odobrenih zakrpi, tako da se označi *checkbox* polje pokraj zakrpe koju se želi povući.
Sigurnosne zakrpe koje međusobno ovise jedna o drugoj potrebno je instalirati zajedno budući da zasebna instalacija nije moguća. Prilikom odobravanja ili povlačenja zakrpi koje ovise o drugim paketima korisniku se prikazuje obavijest koja ga upozorava na međusobnu ovisnost pojedinih paketa. Slično kao i kod sinkronizacije paketa, sve aktivnosti vezane uz odobravanje, odnosno povlačenje zakrpi bilježe se unutar **View approval log** sučelja (Slika 7).



Slika 7: Log zapisi o procesu odobravanja zakrpi

3.4.1.3. Log zapisi

Obzirom da većina aktivnosti vezanih uz održavanje i upravljanje SUS poslužiteljem obuhvaća postupke sinkronizacije zakrpi te njihovog odobravanja i povlačenja, ranije spomenuti log zapis (*Synchronization* i *Approval log*) vrlo je važan element u smislu praćenja i nadzora rada poslužitelja. Osim kroz Web sučelje, isti log zapisi dostupni su i u XML formatu u datotečnom sustavu. U nastavku su navedene informacije koje su dostupne unutar spomenutih log zapisa.

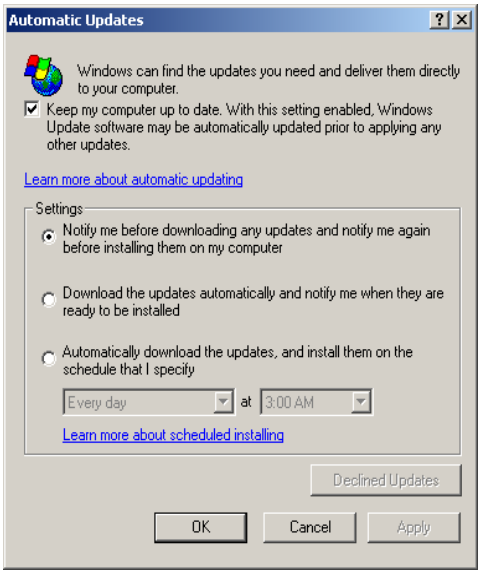
- **Synchronization log**
  - vrijeme posljednje sinkronizacije,
  - vrijeme prve iduće sinkronizacije ukoliko je ista definirana unutar *scheduler* programa,
  - lista paketa koji su dohvaćani/osvježeni u postupku sinkronizacije,
  - lista paketa koji nisu dohvaćani/osvježeni zbog grešaka u procesu sinkronizacije.
- **Approval log**
  - vremena svih promjena nad listom odobrenih sigurnosnih zakrpi,
  - lista elemenata promijenjenih u procesu odobravanja/povlačenja zakrpi,
  - lista svježe odobrenih zakrpi,
  - korisničko ime odgovornog za promjenu.

3.4.2. Podešavanje klijenta

Automatic Updates servis moguće je podešavati lokalno, kroz Automatic Updates aplikaciju unutar Control Panel sučelja, korištenjem Group Policy objekta na razini Windows domene ili izravnim uređivanjem *registry* datoteke. U nastavku su ukratko opisani spomenuti načini podešavanja Automatic Updates klijentske aplikacije.

3.4.2.1. Lokalno podešavanje

Na sljedećoj slici (Slika 8) prikazano je Automatic Updates sučelje za lokalno definiranje postavki servisa.



Slika 8: Sučelje za upravljanje Automatic Updates servisom

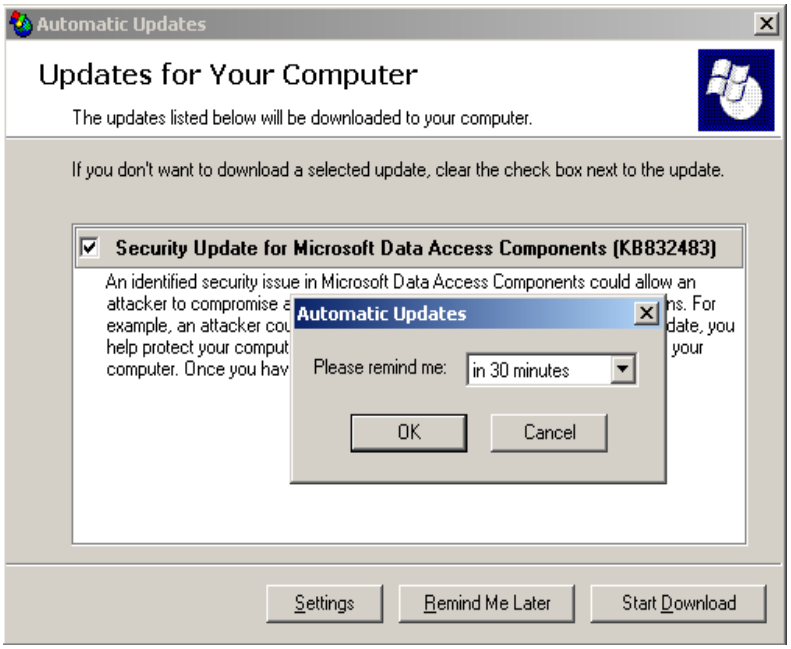
Podešavanjem odgovarajućih postavki, lokalnom se administratoru omogućuje definiranje postavki procesa instalacije sigurnosnih zakrpi. Postoje tri osnovna načina za dohvaćanje i instalaciju zakrpi:

- korisnik se upozorava prije dohvaćanja i prije instalacije svih sigurnosnih zakrpi,
- zakrpe se dohvaćaju automatski, ali se korisnik upozorava prije njihove instalacije,
- zakrpe se automatski dohvaćaju i instaliraju u predefiniranim vremenskim intervalima.

Upozoravanje korisnika provodi se putem odgovarajuće ikone u *system tray* traci računala te se automatski bilježe unutar Event Log aplikacije kako bi se omogućio nadzor sustava.

Kako bi se u što većoj mjeri optimizirao proces instalacije sigurnosnih zakrpi i smanjio utjecaj na aktivnosti korisnika koji je trenutno prijavljen u sustav, Automatic Updates servis koristi tzv. **B**ackground **I**ntelligent **T**ransfer **S**ervice (BITS) pristup koji za dohvaćanje zakrpi koristi isključivo nezauzeti dio komunikacijskog kanala. Ukoliko je sustav podešen tako da se korisnik obavještava prije dohvaćanja i instalacije raspoloživih sigurnosnih zakrpi, lokalnom administratoru, ukoliko je isti prijavljen u sustav biti će prikazano upozorenje u obliku ranije spomenute ikone. Ukoliko lokalni administrator nije trenutno prijavljen u sustav, upozorenje će biti odgođeno do trenutka kada se isti prijavi.

Pritiskom na spomenutu ikonu otvara se sučelje prikazano na sljedećoj slici (Slika 9), pomoću kojeg lokalni administrator može pokrenuti postupak instalacije raspoloživih sigurnosnih zakrpi (kartica **Install**). Pritiskom na karticu **Remind me Latter** moguće je postupak instalacije odgoditi za kasnije.



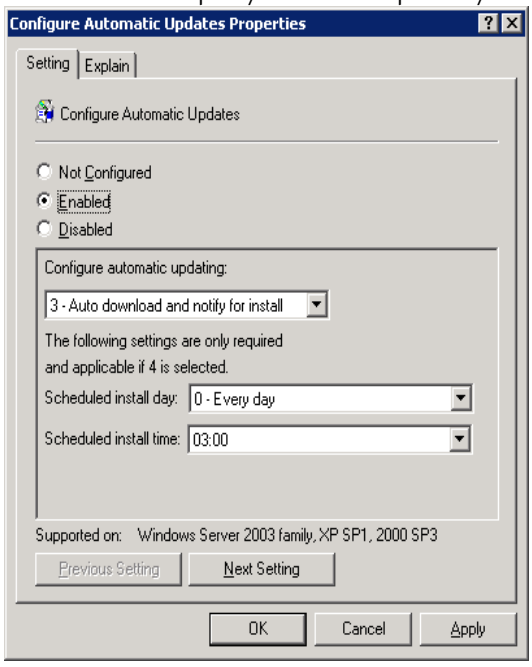
Slika 9: Pokretanje postupka instalacije sigurnosnih zakrpi putem Automatic Updates sučelja

3.4.2.2. Podešavanje putem Group Policy objekta

Osim lokalnog podešavanja, Automatic Updates servis moguće je podesiti i unutar Group Policy objekta unutar Active Directory servisa. Važno je napomenuti da postavke definirane unutar Group Policy sučelja uvijek nadjačavaju one koje su lokalno podešene na korisničkom računalu. Također, u tom slučaju su Automatic Updates postavke unutar Control Panel sučelja onemogućene.

Sučelje za podešavanje Automatic Updates servisa kroz Group Policy prikazano je na sljedećoj slici (Slika 10). Točna putanja u Group policy konfiguraciji je sljedeća:

Computer Configuration/Administrative Templete/Windows Components/Windows Updates.



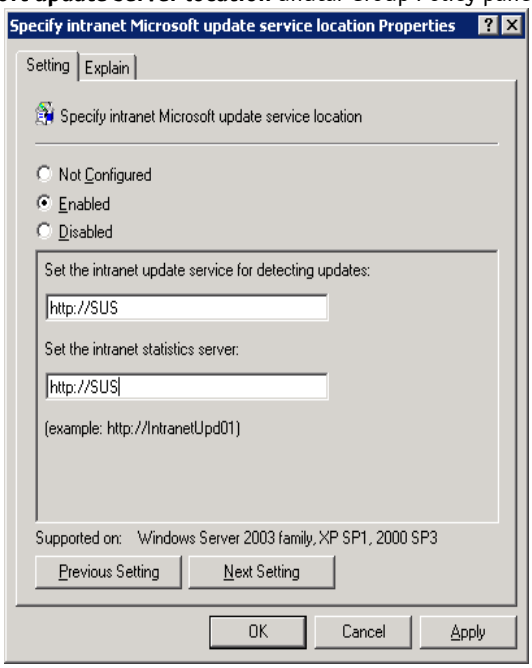
Slika 10: Podešavanje AU servisa putem Group Policy objekta

Nakon što je Automatic Updates servis omogućen odabirom polja **Enabled**, moguće je definirati slične postavke kao što je to opisano kod lokalnog podešavanja:

- **Notify for download and notify for install** - korisnik se upozorava prije dohvaćanja i prije instalacije sigurnosnih zakrpi,
- **Auto download and notify for install** - zakrpe se dohvaćaju automatski, ali se korisnik upozorava prije njihove instalacije,
- **Auto download and schedule the install** - zakrpe se automatski dohvaćaju i instaliraju u predefiniranim vremenskim intervalima.

Schedule opcije moguće je iskoristiti za točno definiranje vremena u kojima će se provoditi automatsko dohvaćanje i instalacija sigurnosnih zakrpi.

Nakon što je omogućen Automatic Updates servis i nakon što su definirane osnovne postavke, potrebno je definirati parametre vezane uz SUS poslužitelj. To je moguće postići unutar sučelja **Specify Intranet Microsoft update server location** unutar Group Policy panela.



Slika 11: Podešavanje parametara SUS poslužitelja

Ukoliko se SUS poslužitelj ne navede svi klijenti će koristiti javne Windows Update poslužitelje.

3.4.2.3. Registry postavke

Postavke Automatic Uopdate servisa moguće je podesiti i izravnim uređivanjem *registry* datoteke sustava. *Registry* parametri vezani uz podešavanje Automatic Updates servisa nalaze se na lokaciji HKLM\Software\Policies\microsoft\Windows\WindowsUpdate\AU, a slijedi opis nekih od njih:

- **NoAutoUpdate** – omogućavanje, odnosno onemogućavanje Automatic Updates servisa.
- **AUOptions** – podešavanje načina rada AU servisa. Moguće su sljedeće vrijednosti:
  - 2 – *notify of download and installation,*
  - 3 – *auto download and notify of installation,*
  - 4 – *auto download and schedule installation*.

  Može se primijetiti da značenje navedenih opcija odgovara onima koje su već ranije opisane kod podešavanja sustava kroz grafičko sučelje. I u ovom slučaju se podrazumijeva da se sva upozorenja prosljeđuju lokalnom administratoru nakon što se prijavi u sustav.
- **ScheduleinstallDay** i **ScheduleInstallTime** – parametri kojima se definira datum i vrijeme automatskog dohvaćanja i instalacije zakrpi.
- **UseWUServer** – omogućuje se korištenje lokalnog SUS poslužitelja ukoliko je parametru pridjeljena vrijednost 1.

- **WUServer** – Ime SUS poslužitelja.

3.4.2.4. Bilježenje log zapisa

Kako bi se omogućilo praćenje rada i nadzor Automatic Update servisa, svi relevantni događaji bilježe se u log datoteke sustava. S obzirom da pravovremena i pouzdana instalacija sigurnosnih zakrpi predstavlja vrlo važan aspekt u pogledu održavanja visoke razine sigurnosti, detekcija bilo kakvih nepravilnosti iznimno je važan korak.
U nastavku su navedeni osnovni tipovi log zapisa kojima je moguće detektirati nepravilnosti u radu Automatic Updates U servisa:

- **Unable to connect** – Problemi u povezivanju sa SUS poslužiteljem, čime je onemogućeno dohvaćanje i instalacija zakrpi. Ovi problemi mogu biti uzrokovani problemima u radu same računalne mreže ili mrežnog sučelja računala putem kojeg je ostvaruje veza, a mogući uzrok mogu biti i problemi s mrežnim postavkama operacijskog sustava.
- **Install ready – no recurring schedule –** dohvaćene zakrpe spremne za instalaciju navedene su kao dio log zapisa. Obavijest o raspoloživim zakrpama biti će prikazana administratoru sustava kada se prijavi u sustav.
- **Install ready –recurring schedule –** dohvaćene zakrpe spremne za instalaciju navedene su kao dio log zapisa. Također je navedeno i vrijeme kada će zakrpe prema definiranim postavkama biti instalirane.
- **Install Success** - poruka o uspješnoj instalaciji zakrpe.
- **Install Failure** – poruka o neuspjeloj instalaciji zakrpe.
- **Restart required – no recurring schedule** – za potpunu instalaciju zakrpi računalo mora biti ponovno pokrenuto. Do sljedećeg *reboot*-a, nije moguće dohvaćanje novih zakrpi.

4. Zaključak

Na temelju provedenih analiza i testiranja, može se zaključiti kako korištenje Microsoft Software Update Services servisa predstavlja iznimno jednostavno i praktično rješenje u pogledu upravljanja sigurnosnim zakrpama u Windows baziranim okruženjima.

Programski paket potpuno je besplatan i može se dohvatiti s Microsoftovih javnih Web stranica. Obzirom na cijenu i funkcionalnosti SUS programskog paketa, može se zaključiti kako isti predstavlja gotovo idealno rješenje za manje informacijske sustave. Ograničenja primjene SUS servisa su njegova nemogućnost instalacije svih tipova sigurnosnih zakrpi. SUS omogućava instalaciju samo kritičnih sigurnosnih zakrpi vezanih uz sigurnosne propuste unutar samog operacijskog sustava. Instalacija zakrpi za upravljačke programe (engl. *device driver*) i aplikacije nije moguća.

Za veće i složenije informacijske sustave koji zahtijevaju potpunu kontrolu i mogućnost kvalitetnijeg upravljanja sigurnosnim zakrpama, zajedno sa naprednijim funkcionalnostima kao što su npr. *change* ili *configuration management* preporučuje se korištenje Microsoftovog System Management Server (SMS) programskog paketa ili komercijalnih rješenja drugih proizvođača.

5. Reference

[1] Microsoft, Software Update Services Overview,
http://www.microsoft.com/windowsserversystem/sus/susoverview.mspx
[2] Microsoft, Software Update Services Deployment,
http://www.microsoft.com/windowsserversystem/sus/susdeployment.mspx