HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Windows XP Service Pack 2 sigurnosna zakrpa

CCERT-PUBDOC-2004-11-98

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

S ciljem podizanja razine sigurnosti Windows XP operacijskog sustava, trenutno jednog od najraširenijeg operacijskog sustava za osobna računala, Microsoft je objavio XP Service Pack 2 sigurnosnu zakrpu koja donosi brojne novitete i poboljšanja u području sigurnosti osobnih računala. Promjene koje SP2 zakrpa donosi kreću se od vrlo jednostavnih nadogradnji, pa sve do značajnih izmjena koje su vezane i uz samu jezgru operacijskog sustava.

Nadogradnjom postojećih, te uvođenjem novih sigurnosnih kontrola Microsoft je pokušao odgovoriti na nove izazove koji se svakodnevno javljaju na polju sigurnosti osobnih računala. Najznačajnije promjene koje SP2 zakrpa donosi vezane su uz unaprjeđenje zaštite od malicioznih programa i napada s Interneta, sprječavanje napada prepisivanjem spremnika (engl. *buffer overflow*), pojačane sigurnosne kontrole unutar alata za pristup sustavu elektroničke pošte i Web-u, efikasniji sustav instalacije sigurnosnih zakrpi i sl. Također, ugrađene su i dodatne funkcionalnosti koje korisnicima i sistem administratorima olakšavaju održavanje sustava i kontrolu sigurnosnih postavki istoga.

Dokument opisuje osnovne karakteristike i promjene koje XP SP2 sigurnosna zakrpa donosi korisnicima Windows XP operacijskih sustava. Ukratko su opisane pojedine sigurnosne kontrole koje dolaze sa ovom zakrpom, način njihovog djelovanja te eventualni problemi koji se mogu javiti nakon njene instalacije.

2. Sigurnosni problemi i zahtjevi

Sigurnosni zahtjevi koji se predstavljaju pred računalne sustave mijenjaju se iz dana u dan. Kontrole koje su prije nekoliko godina u potpunosti zadovoljavale potrebe sigurnosti danas su gotovo neprihvatljive ukoliko se u obzir uzmu svi problemi o kojima je potrebno voditi računa. Sve napredniji maliciozni programi te tehnike i alati koje neovlašteni korisnici koriste prilikom kompromitiranja sustava, postavili su nove i vrlo visoke standarde u pogledu zaštite računalnih sustava.

Danas se poslovanja gotovo u potpunosti baziraju na informatičkoj podršci, a pojavom tehnologija kao što su xDSL i cable modemi i kućna računala su konstantno povezana na Internet. Korištenje Web-a, elektroničke pošte, *instant messaging* servisa i programa za dijeljenje datoteka (engl. *file sharing*) postalo je dio svakodnevnice, pri čemu se vrlo često zanemaruju problemi sigurnosti koji također dolaze sa pojedinim tehnologijama. Dodatni problem svakako predstavlja i nedovoljna edukacija korisnika, što također pridonosi broju računalnih incidenata.

S obzirom na sve navedene probleme osobna računala postala su sve češća meta neovlaštenih korisnika. Iako danas na tržištu postoje brojni sigurnosni alati koji osobna računala štite od prijetnji s Interneta (antivirusna zaštita, osobni vatrozidi i sl.), statistički podaci jasno pokazuju da je broj sigurnosnih incidenata u svakodnevnom porastu. Najveći broj problema uzrokovan je virusima, crvima i drugim sličnim malicioznim programima koji se najčešće šire putem sustava elektroničke pošte, *peer-to-peer* kanala ili putem Web preglednika, a vrlo važnu ulogu igra i neredovito održavanje sustava koje neovlaštenim korisnicima olakšava provođenje malicioznih aktivnosti.

Kao odgovor na ove probleme Microsoft je svojim korisnicima ponudio SP2 sigurnosnu zakrpu za Windows XP operacijske sustave, trenutno jedan od najraširenijih operacijskih sustava za osobna računala. Zakrpa donosi brojna poboljšanja i novitete kojima će se podići razina sigurnosti ovog operacijskog sustava te omogućiti jednostavnije upravljanje istim. Unutar SP2 programskog paketa sadržane su sve dosad objavljene zakrpe za Windows XP operacijski sustav, a također su ugrađene i brojne druge sigurnosne kontrole koje će omogućiti kvalitetniju zaštitu korisničkih računala. Iako je zakrpa dostupna na 25 jezika, Hrvatski jezik zasada nije podržan.

Objava XP SP2 sigurnosne zakrpe jasno ukazuje na novu inicijativu Microsofta, kojoj je cilj korisnicima osobnih računala pružiti veću razinu zaštite te jednostavnije održavanje sustava uz manji utrošak vremena. Pritom se također vodilo računa da se zadrži jednostavnost i fleksibilnost sustava, što ponekada i nije lako s obzirom da sigurnost i funkcionalnost često imaju suprotan predznak. U nastavku dokumenta biti će detaljnije analizirana SP XP2 sigurnosna zakrpa sa pregledom svih značajnijih promjena u odnosu na ranije inačice XP operacijskog sustava.

3. XP SP2 sigurnosna zakrpa

U odnosu na inicijalnu inačicu Windows XP operacijskog sustava, SP2 sigurnosna zakrpa donosi nekoliko potpuno novih i unaprjeđenih sigurnosnih kontrola. Treba naglasiti da one nisu zamišljene kao zamjena za standardne sigurnosne zakrpe i nadogradnje, već kao skup dodatnih sigurnosnih mehanizama kojima će se Windows XP operacijski sustav zaštiti od potencijalnih neovlaštenih aktivnosti.

Na temelju prijašnjih iskustava, u XP SP2 zakrpu ugrađene su one kontrole koje bi korisnike trebale zaštiti od onih prijetnji koje trenutno predstavljaju najveću opasnost za osobna računala, a da se pritom ozbiljno ne naruši fleksibilnost i jednostavnost sustava. Sigurnosne kontrole obuhvaćene XP SP2 sigurnosnom zakrpom mogu se svrstati u nekoliko kategorija:

- unaprjeđena zaštita od malicioznih programa i napada s Interneta (engl. *network protection*),
- unaprjeđena zaštita memorijskog prostora u svrhu sprječavanja izvršavanja malicioznog koda (engl. *memory protection*),
- povećana razina zaštite unutar aplikacija za pristup sustavu elektroničke pošte (engl. *e-mail handling*),
- sigurnije pretraživanje i pristup Internetu (engl. *browser security*),
- održavanje računala (engl. *computer maintenance*).

U nastavku poglavlja dan je kratki pregled navedenih kategorija sa osnovnim sigurnosnim kontrolama koje su u njima javljaju. Kasnije u dokumentu biti će detaljnije opisane pojedine kontrole, njihov utjecaj na sigurnost sustava i navike korisnika.

3.1. Mrežna zaštita

Područje u koje je uloženo najviše truda i na kojem je načinjeno najviše promjena vezano je uz zaštitu računala od napada koji dolaze putem računalne mreže, najčešće javnog Interneta. Ovakav potez posve je logičan budući da se većina sigurnosnih problema za korisnike osobnih računala javlja kao posljedica širenja virusa, crva i brojnih drugih sličnih malicioznih programa. Novosti koje se pojavljuju u SP2 paketu odnose se uglavnom na unaprjeđene funkcionalnosti Windows vatrozida, te promjene unutar RPC (*engl. Remote Procedure Call*) servisa, koji se pokazao kao uzrok brojnih problema kod ranijih inačica Windows operacijskih sustava.

Windows vatrozid je po inicijalnim postavkama automatski uključen, te se njegovo pokretanje vrši vrlo rano u procesu podizanja sustava, prije nego što se inicijalizira mrežni stog i računalo poveže na računalnu mrežu. Ovime se pokušava izbjeći mogućnost napada tijekom podizanja sustava. Na sličan način se sustav nastoji zaštiti i prilikom njegovog zaustavljanja, tako da se vatrozid isključuje vrlo kasno u procesu gašenja, poslije onemogućavanja mrežnog stoga.

Svi portovi su zatvoreni kada nisu u upotrebi, te se kontrola pristupa pojedinim servisima lako može podesiti kroz odgovarajuće korisničko sučelje. Windows vatrozid je u SP2 zakrpi uključen za sva mrežna sučelja, za razliku od ranijih inačica gdje je za svako aktivno sučelje trebalo zasebno podesiti pravila filtriranja mrežnog prometa.

Ozbiljne promjene načinjene su i unutar RPC sučelja. Najznačajnija je ona kojom se inicijalno onemogućava anonimni pristup RPC servisima, a dodane su i nove mogućnosti kontrole pristupa kako bi se omogućila preciznija kontrola koji RPC poslužitelji su blokirani, koji su dostupni samo s lokalne računalne mreže, a koji su dostupni bez ograničenja.

U područje mrežne zaštite spadaju i promjene načinjene na infrastrukturi distribuiranih komponenti objektnog modela, DCOM (*engl. Distributed Component Object Model*). Dodane su nove restrikcije na kontrolu pristupa ovim objektnim modelima kako bi se na taj način smanjio rizik uspješnog provođenja napada putem računalne mreže. Samo autenticirani administratori mogu aktivirati COM komponente, i samo autenticirani korisnici mogu pozivati te iste COM komponente.

3.2. Zaštita memorijskog prostora

Problem zaštite i rukovanja memorijskim prostorom računala vrlo je važan aspekt računalne sigurnosti. Izolacija memorijskog prostora aktivnih procesa te označavanje dijelova memorije unutar

kojih je moguće izvršavati programski kod i onih unutar kojih to nije moguće, iznimno je važno za održavanje visoke razine sigurnosti operacijskog sustava.
Mogućnost prepisivanja podataka u memorijskom prostoru aktivnog procesa proizvoljnim podacima vrlo su opasni i najčešće omogućuju preuzimanje potpune kontrole nad sustavom (ovisno o ovlastima procesa čiji se propust iskorištava). Napadi koji se baziraju na prepisivanju spremnika unutar ranjivog programa s ciljem izvršavanja proizvoljnog programskog koda nazivaju se napadi prepisivanjem spremnika (*engl. buffer overflow*). Iako se statistički gledano najveći broj napada danas bazira upravo na *buffer overflow* ranjivostima, postoje i brojne druge varijante prepisivanja memorijskog prostora koje također mogu rezultirati izvršavanjem proizvoljnog koda na sustavu (npr. *heap overflow*, *format string* napadi, *dtors* tehnika i sl.)
Iako gotovo da ne postoji način da se ovakvi napadi u potpunosti eliminiraju, SP2 sigurnosnom zakrpom pokušava se umanjiti mogućnost njihovog provođenja. Kako se navodi, jedno od poboljšanja na ovom području je ponovno prevođenje sistemskih komponenti jezgre Windows operacijskog sustava kako bi se omogućila detekcija napada prepisivanjem spremnika pohranjenih na stogu.
Zaštita *heap* memorijskog prostora implementira se putem specijalnih kolačića (*engl. cookies*) na temelju kojih je moguće detektirati nedozvoljeno prepisivanje *heap* dijela memorijskog prostora. Ova tehnologija, koju u Microsoftu nazivaju *sandboxing*, tek se treba dokazati kao efikasna metoda sprječavanja neovlaštenih aktivnosti.
Dodatna zaštita memorijskog prostora koju donosi SP2 zakrpa trenutno je omogućena samo na arhitekturama koje podržavaju tehnologiju zaštite izvođenja kôda pod nazivom DEP (*engl. Data Execution Prevention*). Trenutne porodice procesora koje podržavaju DEP tehnologiju su 64-bitni AMD-ov K8, i Intel Itanium. S ciljem da se ova tehnologija proširi, Microsoft surađuje s proizvođačima mikroprocesora, te se očekuje da će ubuduće svi novi 32-bitni i 64-bitni procesori podržavati hardversku zaštitu izvođenja programskog kôda. Ova tehnologija radi na način da procesor sve memorijske lokacije koje ne sadrže izvršni kôd eksplicitno označi kao ne-izvršive. Ovime se osigurava da aplikacija ne izvršava onaj programski kôd koji je ubačen od strane zlonamjernog programa u dio memorijskog prostora označenog kao podatkovni, odnosno ne-izvršiv.

3.3. Zaštita sustava elektroničke pošte

SP2 sadrži i novu inačicu Outlook Express programskog paketa, koji je sada sposoban za blokiranje slika i drugih vanjskih sadržaja u HTML porukama elektroničke pošte. Korisnicima je također omogućeno pregledavanje poruka u čistom tekstualnom (*engl. plain text*) formatu, čime se izbjegava potencijalno nesigurni HTML kôd. Osim navedenog, Outlook Express upozorava kada druge aplikacije pokušavaju poslati poruku elektroničke pošte, te kontrolira otvaranje i pohranjivanje potencijalno zlonamjernih dodataka (*engl. attachment*). Za sigurniju kontrolu dodataka poruka elektroničke pošte, SP2 zakrpa sadrži i AES (*engl. Atachment Execution Control*) aplikaciju, koja omogućuje bolju zaštitu sustava od pokretanja opasnog sadržaja zaprimljenog u prilogu. Osim Outlook Express programa, AES u svom radu koriste i Microsoft Outlook, Windows Messenger, te MSN Messenger programi.

3.4. Sigurnost Web preglednika

Kako bi se omogućio sigurniji pristup i sigurnije pregledavanje Web sadržaja na Internetu, unesena su i nova poboljšanja unutar Internet Explorer Web preglednika. Uključena je provjera dozvola pokretanja izvršnih komponenti, restrikcije na sve URL objekte koje su prije vrijedile samo za ActiveX kontrole, općenito veća kontrola nad svim sadržajima, te zahtjev da svi podaci o tipu datoteke koju pruža Web poslužitelj budu konzistentni. HTML stranicama je dozvoljeno stvaranje samo vlastitih objekata, a ne i pristup već stvorenim objektima pohranjenim u *cache* prostoru. Na ovaj način se malicioznim skriptama onemogućuje prikupljanje povjerljivih korisničkih podataka tijekom pretraživanja Interneta, što je jedna od osnovnih karakteristika različitih spyware i ad-aware malicioznih programa. U Internet Explorer preglednik je integrirano i blokiranje *pop-up* prozora, blokiranje digitalno potpisanog sadržaja od nepovjerljivog autora, te blokiranje sadržaja sa neispravnim digitalnim potpisom.
Posebna pažnja posvećena je postupku osvježavanja računala sigurnosnim zakrpama kako bi se korisnicima ukazalo na iznimnu važnost ovog postupka u sklopu redovitog održavanja. U tu svrhu sa Service Pack 2 zakrpom dolazi i Security Center modul, centralizirano sučelje za analizu informacija o trenutnom stanju računala. Security Center sadrži Windows Update Version 5 program za automatsko

osvježavanje sustava, te Windows Installer 3 program za naprednije sigurnosne opcije u postupku instalacije.

4. Funkcionalnost sustava

Postavlja se pitanje kako se novosti koje donosi XP Service Pack 2 odražavaju na funkcionalnost sustava, na krajnje korisnike, odnosno da li su korisnici prisiljeni promijeniti uobičajene navike, odnosno načine korištenja operacijskog sustava. Iako je većina promjena za krajnjeg korisnika potpuno transparentna, postoje određena područja u kojima će se korisnici, administratori i programeri morati prilagoditi kako bi se u potpunosti iskoristila nova sigurnosna svojstva i karakteristike SP2 sigurnosne zakrpe.

Security Center sučelje će korisnika sustava redovito obavještavati o potencijalnim sigurnosnim nedostatcima i potencijalnim slabostima koje degradiraju sigurnosna svojstva sustava. U ovakve situacije ubrajaju se isključivanje Wndows vatrozida, ignoriranje nadogradnje kritične zakrpe, nedostatak antivirusnog programa ili posjedovanje nedovoljno svježe datoteke s potpisima virusa. Ovakvo ponašanje Security Center sučelja neki će korisnici prepoznati kao dodatni detalj koji unaprjeđuje cjelokupnu sigurnost i praćenje rada sustava, dok će drugi u ovome prepoznati nepotrebnu smetnju koja ometa uobičajeni rad.

Windows vatrozid detektira svaki pokušaj spajanja nove aplikacije na Internet, te se kroz *pop-up* prozor korisniku nudi mogućnost da spajanje omogući ili da to aplikaciji zabrani (Slika 1). Starija inačica vatrozida radila je na sličan način, tako da za će se iskusniji korisnici brzo naviknuti na vatrozidnu zaštitu koja dolazi sa SP2 zakrpom.

Slika 1: Blokiranje spajanja aplikacije na Internet

Scheduled Tasks aplikacija također zahtjeva određeno vrijeme od korisnika kako bi funkcionirala kao i prije instalacije zakrpe. Zadaci koji se ne pokreću pod ovlastima određenog korisnika na sustavu, već su kreirani pod inicijalnim sigurnosnim kontekstom, više ne rade. Korisnici Scheduled Tasks aplikacije morati će obnoviti sve zadatke unosom odgovarajućih zaporki. Ovo je potrebno napraviti samo jednom, tako da i ne predstavlja preveliki problem.

Administratorima je sada omogućena puno bolja kontrola svih aplikacija koje su dostupne na poslužitelju. Nakon instalacije SP2 paketa, biti će nužno postaviti pravila pristupa za aplikacije koje se koriste putem računalne mreže.

Kako su ozbiljne promjene načinjene na RPC servisu i DCOM komponenti, programeri Web i Windows aplikacija morat će provjeriti distribuirane aplikacije koje koriste ove elemente. Povećana je i sigurnost oko ActiveX kontrola, te će programeri koji ih koriste morati analizirati načinjene izmjene kako bi funkcionalnost ostala ista. Web stranice koje se pokreću lokalno, a koriste ActiveX kontrole, također je potrebno doraditi kako bi i ispravno funkcionirale.

Osim navedenih situacija, u kojima se od korisnika zahtjeva određena interakcija kako bi se nastavio daljnji rad, postoje i one koje ne ometaju rad, već samo obavještavaju o izvršenim radnjama. Primjer za ovo moguće je pronaći unutar Internet Explorer Web preglednika, koji prilikom blokiranja *pop-up* prozora o tome javlja obavijest ispod adresnog polja (Slika 2).

Slika 2: Blokiranje pop-up prozora

5. Mrežna zaštita

Novosti koje Service Pack 2 zakrpa donosi na području mrežne zaštite mogu se podijeliti u tri osnovne skupine:

- Windows vatrozid,
- DCOM komponente,
- RPC servis.

U nastavku će biti detaljnije opisani navedeni elementi s njihovim osnovnim karakteristikama.

5.1. Windows vatrozid

Nova inačica Windows vatrozida koja dolazi sa SP2 sigurnosnom zakrpom značajno je unaprjeđena u odnosu na raniju inačicu vatrozida pod nazivom *Internet Connection Firewall*, ili skraćeno ICF. Radi se o softverskom vatrozidu ugrađenom u sam operacijski sustav koji za filtriranje mrežnog prometa koristi *stateful inspection* tehnologiju. Blokiranjem malicioznog i potencijalno opasnog mrežnog prometa, Windows vatrozid korisnicima Windows XP sustava omogućuje zaštitu od prijetnji s Interneta pri čemu su podržani i IPv4 i IPv6 protokoli (za razliku od ICF vatrozida gdje je za filtriranje IPv6 prometa bilo potrebno instalirati *Advanced Networking Pack* paket).
Windows vatrozid radi u tri glavna stanja (Slika 3). On može biti:

- **uključen (engl. on)**

Ovo je ujedno i inicijalna postavka Windows vatrozida za sva mrežna sučelja. Svako novo mrežno sučelje dodano sustavu također biva automatski zaštićeno vatrozidom. Ovo se odnosi i na IPv4 i IPv6 promet, a Windows vatrozid ostaje uključen čak i uz prisutnost drugog vatrozida na sustavu. U ovom načinu rada dozvoljeno je definirati i listu iznimaka. U ranijim inačicama Windows operacijskog sustava, aplikacije su same morale pozivati API sučelje vatrozida kako bi se omogućilo otvaranje odgovarajućeg mrežnog porta neophodnog za komunikaciju s drugim računalima. Aplikacija je također bila odgovorna i za zatvaranje porta nakon kraja komunikacije. Također, aplikacija koja je otvarala mrežni port morala je biti pokrenuta s ovlastima lokalnog administratora kako bi se onemogućilo zaobilaženje sigurnosnih postavki vatrozida.
Sa Service Pack 2 zakrpom, aplikacije kojima mora biti omogućen pristup s mreže mogu se dodati u listu iznimaka vatrozida. Ukoliko je aplikacija na toj listi, vatrozid automatski otvara i zatvara sve portove neophodne za rad aplikacije, bez obzira na ovlasti pod kojima je pokrenuta. Na ovaj način otvoreni su samo neophodni portovi i to samo za vrijeme trajanja komunikacije.

- **uključen bez iznimaka (engl. on with no exceptions)**

Vatrozid može raditi i bez iznimaka, što može biti korisno ukoliko se računalo koristi u manje sigurnim okruženjima (npr. slabo zaštićena bežična mreža, lokalna mreža zaražena virusom ili nekim drugim malicioznim programom i sl.). Treba napomenuti da se prebacivanjem vatrozida u ovaj način rada ne vrši njegova rekonfiguracija. Definirana sigurnosna politika ostaje sačuvana, a vatrozid računalo prebacuje u tzv. izolaciju. Svi mrežni portovi se zatvaraju i sve postojeće veze bivaju prekinute. Svi zahtjevi aplikacija za otvaranjem portova se ignoriraju. Na ovaj način računalo je zaštićeno od svih potencijalnih mrežnih napada.

- **isključen (engl. off)**

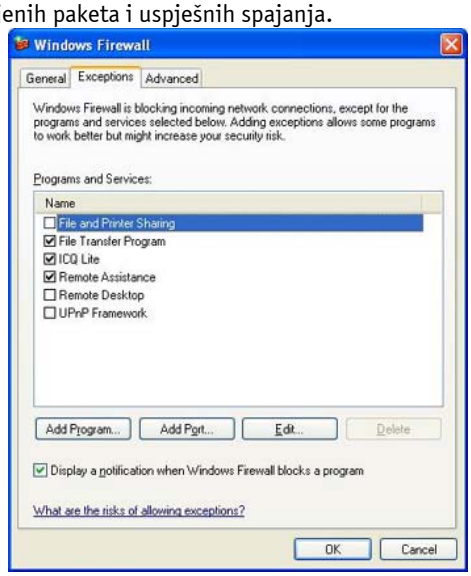
Posljednje stanje vatrozida je ono u kojem je on onemogućen. Ovo stanje se može koristiti prilikom dijagnosticiranja potencijalnih problema vezanih uz rad vatrozida ili u nekim drugim specifičnim

uvjetima koji zahtijevaju njegovo onemogućavanje. U normalnom radu svakako se preporučuje ostaviti vatrozid u inicijalnom stanju, odnosno omogućiti ga. Sučelje za odabir stanja Windows vatrozida prikazano je na sljedećoj slici (Slika 3).

Slika 3: Odabir glavnih stanja vatrozida

Mogućnosti podešavanja Windows vatrozida su slijedeće:

- omogućavanje statičkih iznimki za pojedine aplikacije (Slika 4).
- konfiguracija osnovnih ICMP opcija.
- bilježenje odbijenih paketa i uspješnih spajanja.



Slika 4: Lista iznimki vatrozida

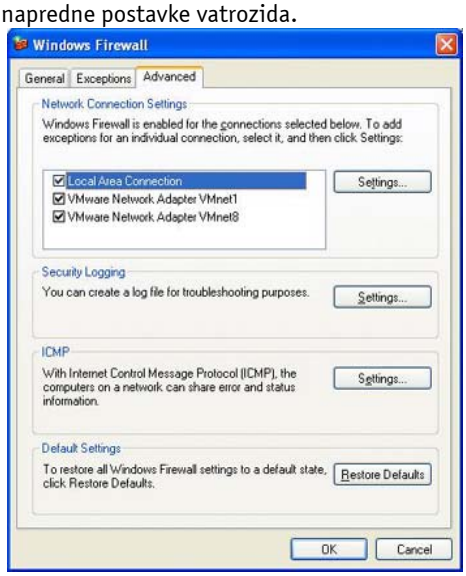
Kako je već ranije spomenuto, pokretanje vatrozida obavlja se vrlo rano u fazi podizanja sustava, čime se povećava njegova učinkovitost s obzirom da se smanjuje mogućnost neovlaštenog pristupa tijekom pokretanja sustava. U ranijoj inačici Windows operacijskog sustava postoji kratak vremenski period između osposobljavanja mrežnog stoga i pokretanja ICF vatrozida. Ovakav slijed aktivnosti računalo ostavlja nezaštićenim u kratkom vremenskom periodu, što je predstavljalo određeni sigurnosni propust.

U okviru Windows XP SP2 zakrpe, IPv4 i IPv6 vatrozid sadrži predefiniranu sigurnosnu politiku koja se primjenjuje tijekom podizanja sustava. Politika se naziva *boot-time* sigurnosna politika. Prilikom

pokretanja vatrozid dozvoljava usko ograničeni broj servisa, DHCP, DNS, te komunikaciju s domenskim poslužiteljem. Nakon što je vatrozid omogućen, primjenjuje se sigurnosna politika vatrozida, a *boot-time* politika se uklanja. Za administraciju vatrozida i sigurnosne politike dostupno je grafičko sučelje, dok modifikacija *boot-time* politike nije moguće. Ovakvom arhitekturom umanjuje se mogućnost kompromitiranja sustava tijekom njegovog podizanja.
Ukoliko se Windows vatrozid zbog određenih problema ne pokrene, *boot-time* politika ostaje vrijediti. Svi pokušaji spajanja na računalo su blokirani. U ovom slučaju administratoru nije omogućeno uklanjanje problema putem računalne mreže budući da su svi mrežni portovi zatvoreni. Kako bi se isključila *boot-time* politika potrebno je zaustaviti Windows firewall servis i promijeniti njegovo pokretanje u ručno (engl. *manual*) ili ga u potpunosti onemogućiti (engl. *disable*).
Filtriranje prometa provodi se tako da se zabranjuje sav nedozvoljen promet prema računalu (engl. *incoming*), dozvoljava se sav promet prema van (engl. *outcoming*), te se automatski prihvaćaju svi paketi koji su dio konekcije inicirane sa računala na kojem je vatrozid pokrenut.
Filtriranje se obavlja provjerom stanja u kojem se paket nalazi i provjerom konteksta sjednice. Tri su osnovna pravila na kojima se bazira sigurnosna politika:

- svi paketi koji su dio ranije inicirane sjednice automatski se propuštaju,
- svi paketi koji su dio novo inicirane konekcije, bilježe se interno u tablici aktivnih konekcija, te se prosljeđuju dalje.
- svi dolazni paketi koji ne pripadaju ranije iniciranoj konekciji se blokiraju.

Ova jednostavna pravila osiguravaju nesmetan pristup Internetu, dok se sve neovlaštene konekcije prema računalu blokiraju. Naravno, ovako definiranim pravilima moguće je pridijeliti određene iznimke kako bi se omogućio nesmetan rad mrežnih aplikacija čiji način rada odstupa od navedenih pravila.
Vatrozid podržava i definiranje grupnih politika, koje omogućuju centralizirano upravljanje računalima unutar Windows domene. Sigurnosnu politiku može definirati i lokalni korisnik, međutim ukoliko postoji grupna politika ona ima prednost i lokalni korisnici nemaju prava modifikacije postavki vatrozida.
U naprednim postavkama (kartica **Advanced**) nude se i dodatne mogućnosti podešavanja vatrozida, (Slika 5). Ukoliko računalo ima više mrežnih sučelja, vatrozid je po inicijalnim postavkama omogućen na svima njima. U prijašnjim inačicama vatrozida svako mrežno sučelje imalo je svoju zasebnu politiku što je otežavalo administraciju vatrozida i povećavalo mogućnost pogreške. Također, nije postojala mogućnost da novo definirana sučelja preuzmu postavke primijenjene na postojećim sučeljima. Sa globalnom konfiguracijom svaka promjena se promovira na sve mrežne konekcije, te i one nove automatski usvajaju istu konfiguraciju. Ukoliko je potrebno za svako sučelje konfigurirati drugačiju politiku i to je moguće kroz napredne postavke vatrozida.



Slika 5: Napredne postavke vatrozida

Ako je računalo spojeno na domenu, moguće je definirati i različite profile vatrozidne zaštite. Moguće je definirati posebnu sigurnosnu politiku u slučaju kada je računalo spojeno u lokalnu računalnu mrežu kojoj se u određenoj mjeri vjeruje, te druge politike kada to nije slučaj. Za prijenosna računala ovo je vrlo praktična mogućnost. Naime, za takva računala poželjno je imati više sigurnosnih politika vatrozida koje su primjenjive na različita okruženja u kojima se računalo koristi. Konfiguracija koja zadovoljava sigurnosne zahtjeve povezivanja računala na lokalnu računalnu mrežu može biti potpuno neprikladna ukoliko se računalo koristi za pristup Internetu.
Vatrozid vrši i detaljno bilježenje aktivnosti u log datoteke sustava sa detaljnim informacijama o blokiranim paketima, uspješnim i neuspješnim spajanjima i sl. Bilježenje log zapisa vrlo je važno kako bi se omogućilo praćenje rada i nadzor sustava.

5.2. RPC servis

RPC (*engl. Remote Procedure Call*) je servis koji omogućuje razmjenu poruka i povezivanje udaljenih računala. Na ovaj način se aplikaciji na jednom računalu omogućuje korištenje servisa koji se nalaze na drugim računalima na mreži. Na lokalnim računalnim mrežama RPC servis nalazi svoju primjenu kod udaljene administracije, dijeljenja datoteka i printera, te izradi distribuiranih aplikacija. Samim time može se zaključiti kako bi ovih promjena uglavnom trebali biti svjesni programeri RPC aplikacija i sistem administratori. Za obične korisnike ove promjene su prilično transparentne.
Windows XP operacijski sustav posjeduje RPCSS podsustav, koji je zadužen za označavanje pristupnih točaka dostupnih servisa i koji ujedno aplikacijama omogućuje pristup spomenutim točkama. Osim ovog podsustava, za ispravno funkcioniranje neophodan je i servis pod nazivom `rpclocator` koji distribuiranim aplikacijama pomaže u pronalaženju drugih aplikacija na mreži koje su dostupne i sposobne odgovoriti na tražene zahtjeve.
Problem koji se javljao u vezi s RPC servisima proizlazio je iz činjenice da Windows XP operacijski sustav ima preko 60 servisa, baziranih na RPC protokolu. Iz samog broja pokrenutih servisa jasno se može zaključiti da su oni predstavljali vrlo široko područje koje su zlonamjerni korisnici mogli iskoristiti za provođenje neovlaštenih aktivnosti. Pristup koji je bio korišten u starijim inačicama vatrozida bio je potpuno blokiranje svih RPC komunikacija. Ovo je upravo i jedan od razloga zašto mnogi korisnici nisu koristili ICF vatrozid. Pri njegovom radu bilo je onemogućeno dijeljenje datoteka i printera, te rad brojnih drugih servisa što je većini korisnika bilo neprihvatljivo rješenje.
Prilikom pokušaja spajanja RPC servisa, Windows vatrozid prihvatit će konekciju samo ukoliko je proces pokrenut u okviru sigurnosnog konteksta lokalnog sustava, mrežnog servisa, ili lokalnog servisa. Na ovaj način smanjuje se mogućnost spajanja malicioznih programa koji se lažno predstavljaju kao legitimni RPC servisi.
Uz sve nabrojano, RPC servisi doživjeli su još jednu značajnu promjenu, a ta je da se njihovo korištenje ograničava samo na lokalne i autenticirane korisnike. Za podešavanje ove funkcionalnosti zadužen je registry ključ `RestrictRemoteClients`. Preko njega administratori mogu smanjiti inicijalne kontrole koje sve udaljene anonimne pozive upućene RPC servisima odbijaju.

5.3. DCOM sustav

Microsoft *Distributed Component Object Model* (COM) je distribuirani, objektno orijentirani sustav za kreiranje izvršnih komponenti koje mogu međusobno surađivati. DCOM omogućava distribuiranost aplikacija po različitim lokacijama kako je to najpogodnije za korisnike i pojedine aplikacije. DCOM protokol transparentno pruža podršku za pouzdanu i sigurnu komunikaciju između COM komponenti.
Iako mnoge COM aplikacije posjeduju specifičan dio programskog kôda koji se odnosi na sigurnost, one vrlo često koriste oslabljenje postavke koje dozvoljavaju neautenticirani pristup procesima. U ranijim inačicama Windows operacijskog sustava nije postojao način da se ove postavke izmjene kako bi se podigla razina sigurnosti sustava.
COM infrastruktura se oslanja na već spomenuti RPCSS podsustav, koji u ovom slučaju služi za aktiviranje COM objekata i održavanje tablice sa aktivnim objektima. Ovaj servis otkriva RPC sučelja kojima se može pristupiti. Ako neki od COM poslužitelja dozvoljavaju neautenticirani udaljeni pristup, bilo koji korisnik može pristupiti tim sučeljima, što automatski otvara mogućnost napada na RPCSS sustav.

Također nije bilo moguće odrediti razinu izloženosti COM poslužitelja na računalu. Ona se mogla odrediti samo kroz sustavni pregled svih registriranih COM aplikacija. Kako je njih u inicijalnoj instalaciji Windows XP operacijskog sustava bilo oko 150, taj zadatak je predstavljao ozbiljan problem. Nove DCOM restrikcije umanjuju spomenute probleme. Administratoru se pruža mogućnost i onemogućavanje DCOM aktivacije i poziva.
Inicijalno su svim korisnicima na sustavu omogućene lokalne akcije, čime se osigurava nesmetan rad bez ikakvih softverskih promjena ili izmjena na operacijskom sustavu. Svima je također omogućen udaljeni poziv, dok je udaljena aktivacija COM poslužitelja omogućena samo administratorima.
Sve promjene koje su načinjene na ovom dijelu Windows XP operacijskog sustava odnose se samo na one korisnike koji koriste COM aplikacije kao poslužitelje, a više o ovoj temi moguće je pronaći na službenim Web stranicama Microsofta.

5.4. Alerter i Messenger servisi

Alerter i *Messenger* servisi su komponente Windows operacijskog sustava koje omogućuju jednostavnu razmjenu poruka između računala na računalnoj mreži. *Messenger* servis prosljeđuje poruke između različitih aplikacija i servisa, dok je *Alerter* servis namijenjen obavijestima od strane administratora. Bitno je napomenuti da se ovi servisi koriste samo na računalima koja su povezana u lokalnu računalnu mrežu.
Administratori i programeri koji koriste spomenute servise trebali bi se detaljnije upoznati s promjenama koje donosi Service Pack 2 zakrpa. Jedina promjena koju su ova dva servisa doživjela je ta da su oni inicijalno onemogućeni.
Kada su navedeni servisi pokrenuti, dozvoljavaju spajanja na računalo, te samim time predstavljaju potencijalnu prijetnju. Osim toga analize su pokazale da njihovo korištenje i nije toliko učestalo. Iz ova dva razloga odlučeno je da sa Service Pack 2 zakrpom ovi servisi više neće biti inicijalno pokrenuti.

5.5. Dodatne promjene

Osim upravo obrađenih područja koja su doživjela značajnije promjene unutar Service Pack 2 zakrpe, postoje dodatni segmenti koji su također u određenoj mjeri izmijenjeni. U ovom poglavlju ukratko će biti predstavljeni neki od njih.

5.5.1. Bluetooth podrška

Bluetooth je bežična tehnologija kratkog dometa koja omogućuje povezivanje mobilnih uređaja. Tehnologija je postala iznimno popularna i danas se koristi kod velikog broja uređaja (mobilni uređaji, dlanovnici i sl.). Nakon objave SP2 zakrpe korisnicima XP operacijskog sustava na raspolaganje je stavljena mogućnost korištenja *bluetooth* tehnologije.
U tom smislu Service Pack 2 zakrpa omogućuje sljedeće funkcionalnosti:

- povezivanje Bluetooth uređaja na računalo,
- stvaranje bežičnog okruženja uz pomoć Bluetooth miša i tipkovnice,
- prijenos datoteka između računala i Bluetooth uređaja,
- ispis na Bluetooth printeru,
- spajanje računala na računalnu mrežu ili Internet putem Bluetooth mobilnog telefona,
- uspostava IP konekcije na Internet pomoću Bluetooth mobilnog telefona.

Uz dostupnost prikladnih programa na Windows XP operacijskom sustavu moguće je izvršavati i druge operacije sa *Bluetooth* uređajima:

- sinkoronizacija adresara i kalendara sa Bluetooth mobilnim telefonom ili dlanovnikom,
- čitanje koordinata sa GPS uređaja.

Ukoliko na sustavu nije dostupan *Bluetooth* odašiljač, ne postoje nikakve promjene u ponašanju sustava. Kada je odašiljač prisutan i Bluetooth podrška aktivna, u Control Panel sučelju pod **Network Connections** sekcijom pojavljuje se opcija pod nazivom Bluetooth Devices.

5.5.2. Alati za administraciju klijenata

Alati za administraciju klijenata dio su Microsoft MMC konzole za upravljanje (*engl. Microsoft Management Console*), a omogućuju administraciju korisničkih računa, računala i servisa na lokalnim ili udaljenim računalima. Za upravljanje ovim resursima koriste se dva sučelja:

- **Select Users, Computers, or Groups,**

Koristi se prilikom sastavljanja pristupnih lista za dijeljene direktorije, odabir udaljenog računala nad kojim obavljaju aktivnsti te upravljanje lokalnim korisničkim računima i grupama.

- **Find Users, Computers, or Groups,**

Koristi se pri pretraživanju Active Directory imenika u My Network Places postavkama i traženju printera za Add Printer Wizard opciju.

Kako bi se ovim alatima omogućilo povezivanje na udaljeno računalo, računalo mora imati otvoren 445 TCP port. U inicijalnim postavkama ovaj port nije otvoren, što će uzrokovati greške prilikom pokušaja spajanja na udaljeno računalo. Kako bi se riješio problem, na udaljenom računalu potrebno je omogućiti komunikaciju prema TCP 445 mrežnom portu.

5.5.3. TCP/IP

TCP/IP skup standardnih protokola za komunikaciju između udaljenih računala također je unutar Service Pack 2 zakrpe doživio određene preinake. Implementacija ovih protokola i dalje podržava primanje prometa na tzv. *raw* IP mrežnim utičnicama (engl. *sockets*), međutim slanje paketa je ograničeno na dva načina:

- TCP podaci se ne mogu slati preko *raw* mrežnih utičnica,
- UDP paketi s neispravnom odredišnom adresom ne mogu se slati preko *raw* mrežnih utičnica. IP adresa svakog UDP paketa koji se šalje mora postojati na mrežnom sučelju ili paket neće biti moguće proslijediti.

Ove preinake trebale bi umanjiti mogućnost provođenja distribuiranog napada uskraćivanjem računalnih resursa (engl. *distributed denial of service*), te mogućnost lažiranja mrežnih paketa (engl. *spoofing*).

Dodatna novost je ograničavanje simultanih pokušaja uspostave TCP konekcija. Nakon što se dosegne predefinirana granica, svi daljnji pokušaji spajanja stavljaju se u red te se razrješavaju u konstantnim vremenskim razmacima. Ovakvom arhitekturom ograničava se brzina kojom se zlonamjerni programi, kao što su virusi, crvi i sl. šire računalnom mrežom. Spomenuti programi vrlo često pokušavaju doći do drugih računala otvarajući simultane konekcije prema slučajno odabranim IP adresama. Većina ovih pokušaja rezultira neuspjelim spajanjima, tako da se ubrzo postiže ograničenje pokušaja, te se pojavljuje novi proces pod ID oznakom 4226. On je znak da je na sustavu aktivna aplikacija koja pokušava otvoriti prevelik broj nelegitimnih konekcija, te ju je potrebno onesposobiti.

Opisane promjene također mogu utjecati na određene sigurnosne alate. Alati za pregledavanje mrežnih portova (kao što je npr. nmap) mogli bi zbog opisanih promjena funkcionirati nešto sporije, a primijećeni su i ozbiljniji problemi kao što je potpuna nemogućnost njihovog korištenja.

6. Zaštita memorijskog prostora

Kako bi se u što većoj mjeri osigurala zaštita memorijskog prostora, u Microsoftu su odlučili uvesti tehnologiju zaštite izvođenja programskog kôda, odnosno tehnologiju prevencije izvođenja programskog kôda na memorijskim stranicama rezerviranim za podatke, DEP (*engl. Data Execution Prevention)*. DEP tehnologija je u Sevice Pack 2 zakrpi ostvarena i hardverski i softverski.

Hardverski DEP označava sve memorijske lokacije u procesu kao ne-izvršive ukoliko te lokacije eksplicitno ne sadrže izvršni programski kôd. Postoji grupa napada koja se provodi ubacivanjem i pokretanjem izvršnog kôda iz ne-izvršivih memorijskih područja. DEP pomaže pri sprječavanju takvih napada tako da ih pokušava pravovremeno detektirati te spriječiti njihovo daljnje izvršavanje.

Glavna prednost ovakvog oblika zaštite je sprječavanje izvršavanja programskog kôda iz memorijskih stranica rezerviranih za podatke kao što su stog (*engl. Stack*) i *heap* memorijski prostor. U normalnom okruženju programski kôd se ne izvodi s ovih lokacija. Hardverski DEP detektira izvođenje kôda s ovih lokacija te generira iznimku. Ukoliko se iznimka ne obradi proces se terminira. Iako se obustavljanje procesa ne čini kao idealno rješenje, ovakav pristup ipak sprječava izvršavanje potencijalno

zlonamjernog programskog kôda. Treba napomenuti da bi određene aplikacije mogle biti nekompatibilne s zaštitom izvođenja programskog kôda, pri čemu se prvenstveno misli na aplikacije koje koriste dinamičko generiranje kôda bez eksplicitnog davanja ovlasti izvršenja upravo generiranog kôda.

Hardverski DEP se oslanja na sposobnost procesora da označi memoriju odgovarajućim atributom koji označava da se nikakav programski kôd ne bi smio izvršavati s tog područja memorije. DEP se bazira na virtualnim memorijskim stranicama mijenjajući bit u tablici stranica memorije kojim označava stranicu kao ne-izvršivu. Hardverska implementacija ovog procesa varira o arhitekturi procesora. Svaki procesor koji podržava hardverski DEP je sposoban generirati iznimku prilikom pokušaja izvršavanja programskog kôda s memorijskih lokacija kojima je odgovarajući atribut označen.

Advanced Micro Devices (AMD) i Intel posjeduju porodice procesora koje posjeduju odgovarajuću arhitekturu kako bi bili kompatibilni s DEP tehnologijom. U Microsoftu vjeruju da će svi budući 32-bitni i 64-bitni procesori podržavati ovu tehnologiju.

Kako bi se memorija zaštitila i na postojećim 32-bitnim procesorima koji trenutno ne podržavaju hardverski DEP, Service Pack 2 provjerava stog i *heap* memoriju i softverskim putem. Stog je memorijski prostor koji se koristi za privremene lokalne varijable. Prostor za stog se automatski alocira prilikom poziva funkcija, i oslobađa se kada funkcija završi s izvođenjem. *Heap* memorija koristi se za dinamičko alociranje i oslobađanje memorije za podatke koji će imati nešto duži životni vijek.

S ciljem zaštite stoga, sve sistemske izvršne datoteke ponovno su prevedene koristeći opciju koja omogućava sigurnosne provjere sistemskog stoga. Nekoliko dodatnih instrukcija pri pozivu funkcija i njihovom vraćanju rezultata omogućava prepoznavanje većine pokušaja prepisivanja sistemskog stoga.

S ciljem zaštite *heap* memorijskog prostora, dodani su tzv. "kolačići" (*engl. cookies*). Ovi specijalni markeri dodaju se na početak i kraj svakog alociranog dijela memorije koji se koristi kao *heap* memorijski prostor. Oni se pregledavaju pri svakom alociranju i oslobađanju memorije, te je na taj način, kroz nedostatak ili nekonzistentnost kolačića, moguće uočiti potencijalne pokušaje neovlaštenog prepisivanja memorijskog prostora.

7. Sigurnija obrada elektroničkih poruka

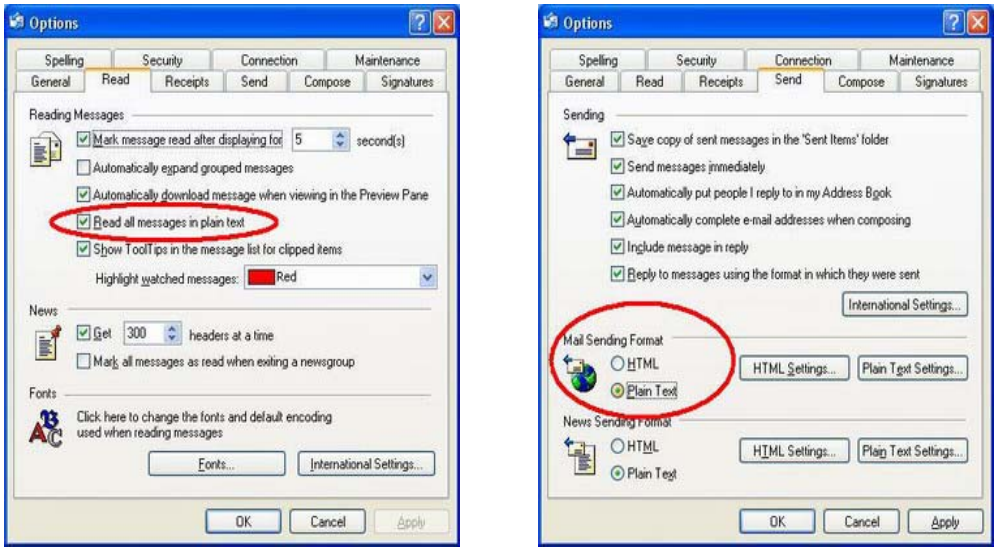
Najveći broj malicioznih programa širi se putem elektroničke pošte (najčešće u obliku dodataka) i *instant messaging* aplikacija. Kako bi se sustav i u ovom smislu zaštitio od malicioznih aktivnosti učinjene su značajne promjene u načinu primanja i obrade spomenutih poruka. Promjene se prije svega odnose na Outlook Express programski paket, a nove kontrole dodane su i Windows Messenger servisu.

Neki dodaci, kao što su npr. poruke u čistom tekstualno obliku (engl. *plain text*) i jednostavne slike mogu se unaprijed prepoznati kao sigurne. Izvršne datoteke se inicijalno smatraju rizičnima, dok zip datoteke i drugi oblici arhiva, iako su sami po sebi sigurni, mogu sadržavati potencijalno zlonamjerne sadržaje.

7.1. Outlook Express

Jedna od glavnih novosti kod navedenog programskog paketa je mogućnost pregledavanja primljenih poruka elektroničke pošte u tekstualnom obliku. Do sada su se poruke mogle pregledavati samo u *Hypertext Markup Language* (HTML) načinu rada, što je obavljala MSHTML kontrola. Za tekstualno pregledavanje poruka zadužena je *rich edit* kontrola koja predstavlja prepreku pri pokušaju izvođenja zlonamjernog kôda sadržanog u poruci elektroničke pošte. Računala s ranijom inačicom XP Windows operacijskog sustava bila su izložena opasnosti budući da je Outlook Express programski paket procesirao skripte sadržane u HTML zaglavljima poruka s HTML sadržajem. MSHTML kontrola je skripte automatski izvršavala, za razliku od *Rich Edit* kontrole koja to ne čini. Kako tekstualne poruke elektroničke pošte ne zahtijevaju obradu HTML zaglavlja, gotovo da i nema vidljive razlike kod standardnih formata poruka.

Prilikom tekstualnog načina rada s Outlook Expressom slijedeće opcije nisu moguće: promjena veličine fonta i pretraživanje sadržaja poruke. Podešavanje ovog načina rada obavlja se kroz izbornik prikazan na sljedećoj slici (Slika 6), a do njega je moguće doći kroz **Tools** padajući meni odabirom opcije **Options**.



Slika 6: Odabir čitanja i slanja mail poruka u tekstualnom formatu

Osim tekstualnog načina rada Outlook Express korisnicima olakšava i suzbijanje *spam* poruka. Kako bi provjerili valjanost e-mail adrese, *spammeri* vrlo često koriste specijalne HTML poruke koje prilikom otvaranja kontaktiraju određeni Web poslužitelj s ciljem da prikažu dodatni vanjski sadržaj. Poruke elektroničke pošte vrlo često sadrže slike vrlo malih veličina koje se nakon što se poruka otvori spajaju na javne Web poslužitelje s namjerom da dohvate i prikažu sliku. Web poslužitelj registrira mail adresu poruke kao valjanu i ona se kasnije koristi kao odredište za slanje spam poruka. Ukoliko je opcija *Block images and other external content in HTML e-mail* omogućena, ponašanje Outlook Express programa mijenja se na taj način da se ne vrši spajanje na vanjske Web poslužitelja sa svrhom prijenosa dodatnog sadržaja (Slika 7). Ova opcija je inicijalno uključena u Service Pack 2 zakrpi.

Slika 7: Podešavanje sigurnosnih opcija unutar Internet Explorera

Prema dokumentaciji proizvođača, postoje još mnoga područja na kojima je Outlook Express programski paket izmijenjen kako bi korisnicima pružio veću razinu sigurnosti. Međutim te promjene su za korisnike pretežno transparentne.

7.2. AES aplikacija

Windows XP Service Pack 2 zakrpa sadrži i poseban servis za kontrolu izvršavanja priloga poruka pod nazivom AES (*engl. Attachment Execution Service*). Ovaj servis omogućuje kontrolu pregledavanja i izvršavanja datoteka primljenih kroz priloge poruka elektroničke pošte. AES posjeduje COM sučelje te ga koriste razni programi na sustavu, a prije svega se to odnosi na Outlook Express i Windows Messenger programske pakete.

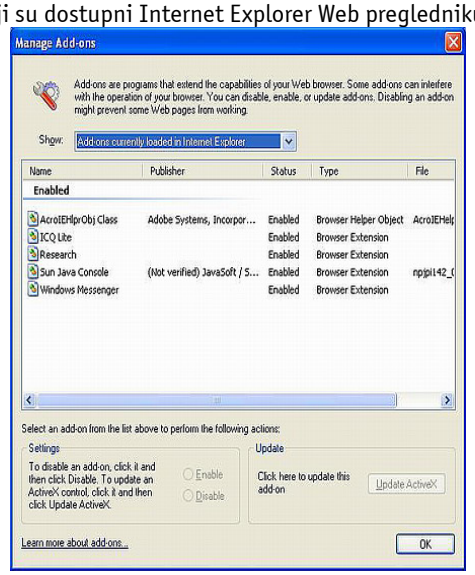
AES zaštita funkcionira tako da primljene datoteke provjerava na više načina. Prvo što se provjerava je ekstenzija primljene datoteke. Unaprijed je definirano da su neki tipovi datoteka sigurni, kao što su tekstualne datoteke (.txt), JPEG i GIF zapisi (.jpg, .gif). Provjerava se i MIME tip te se uspoređuje konzistentnost. Na temelju ove asocijacije i postojeće liste odlučuje se da li se radi o potencijalno opasnoj datoteci ili ne. AES također provjerava da li je aktivan antivirusni program, te da li je datoteka s potpisima virusa aktualna prije nego što se dozvoli otvaranje nesigurnog priloga.

Prilikom otvaranja poruke elektroničke pošte s prilogom, Outlook Express program poziva AES modul kako bi se utvrdilo da li je sadržaj priloga siguran. Ako je prilog siguran, on će u potpunosti biti vidljiv korisniku. Ukoliko je sadržaj priloga nesiguran, kao što je izvršna datoteka, korisnik neće biti u mogućnosti otvoriti prilog, već će dobiti obavijest o blokiranju. U situacijama kada AES ne može utvrditi da li je prilog siguran ili ne, korisniku se otvara obavijest o tome da je datoteka koju pokušava otvoriti potencijalno opasna za njegov sustav. Ukoliko se nastavi s otvaranjem datoteke, pokreće se aktivni antivirusni program.

Windows Messenger servis radi na sličan način prilikom operacija s dodacima. Jedina razlika u odnosu na poruke elektroničke pošte je ta što je ovdje neophodna korisnička suglasnost za prijenos datoteka na sustav, dok se poruke elektroničke pošte automatski prenose.

8. Sigurnije pretraživanje Interneta

Iako dodaci (*engl. Add-ons*) Internet Explorer Web pregledniku imaju namjenu da olakšaju i ubrzaju korištenje i pretraživanje Interneta, mnogi od njih znaju korisnicima stvarati probleme. Pod dodacima misli se na razna proširenja preglednika, te ActiveX kontrole. Nova inačica Internet Explorer programa koja dolazi sa Service Pack 2 zakrpom omogućava kontrolu dodataka, te detekciju nasilnog prekida rada uzrokovanu nekim od dodataka. Opcija za podešavanje dodataka omogućava korisnicima pregled i kontrolu svih dodataka koji su dostupni Internet Explorer Web pregledniku (Slika 8).



Slika 8: Konfiguracija dodataka Internet Exploreru

Prilikom otvaranja Web stranice, Internet Explorer postavlja ograničenja na moguće akcije učitanih stranica. Ograničenje se nameće ovisno o lokaciji Web stranice. Ukoliko se stranica nalazi na javnom Internetu, ona neće imati iste ovlasti izvršavanja određenih operacija kao što su npr. čitanje sadržaja na lokalnom računalu. Web stranice koje se nalaze lokalno na računalu smještene su u **Local Machine**

zone sigurnosnu zonu gdje su restrikcije najslabije. **Local Machine** zona je jedna od sigurnosnih zona Internet Explorera Web preglednika ali ona nije prikazana u njegovim postavkama.
Sa Service Pack 2 zakrpom, sve lokalne datoteke i sav sadržaj se procesira sa sigurnosnim kontekstom **Local Machine** zone. Ove se razlikuje u tome što se prije sav sadržaj smatrao sigurnim, te se na njega nisu postavljala nikakva ograničenja. Unutar **Local Machine** zone HTML sadržaj pregledavan kroz Internet Explorer posjeduje određena ograničenja, čime se smanjuje vjerojatnost uspješnog provođenja napada zlonamjernim HTML kôdom korištenjem **Local Machine** zone. Jedna od restrikcija je ta da se ActiveX skripte unutar HTML stranica više ne pokreću. Skripte sada od korisnika moraju zatražiti dozvolu za svoje izvršenje (Slika 9).

Slika 9: Blokiranje ActiveX skripti unutar Internet Explorera

Prilikom prijenosa datoteka s Web poslužitelja, Internet Explorer Web preglednik provjerava slijedeće informacije:

- ekstenziju datoteke,
- tip sadržaja iz HTTP zaglavlja,
- Content-Dispositon HTTP zaglavlje,
- MIME tip.

Internet Explorer zahtjeva da su sve ove informacije koje daje Web poslužitelj konzistentne. Ukoliko dođe do neslaganja prilikom provjere, Internet Explorer mijenja ekstenziju datoteke.
Internet Explorer također koristi već ranije spomenuti AES servis za provjeru sigurnosti dohvaćenih datoteka. Korisniku se kroz dijaloške prozore pruža znatno više informacije o datoteci nego što je to bio slučaj u ranijim inačicama. Uz izvor, tip i veličinu datoteke, sada se pruža i informacija o izdavaču softvera koji se pokušava instalirati, te se izdaje upozorenje ukoliko se radi o programskom paketu nepoznatog izdavača (Slika 10).

Slika 10: Pokretanje datoteke nepoznatog izdavača

U posljednje vrijeme *pop-up* prozori postali vrlo su popularan način oglašavanja na Internetu. Nova inačica Internet Explorer Web preglednika sadrži ugrađenu kontrolu i mogućnost blokiranja *pop-up* prozora. Internet Explorer blokira gotovo sve neželjene *pop-up* prozore. Iako ova kontrola Internet Explorer programa radi vrlo dobro, već odavno gotovo svi napredniji Internet preglednici posjeduju ovakve odlike, te je već i bilo vrijeme da ovu mogućnost ponudi i Microsoft u svom proizvodu.
Osim još nekih sigurnosnih poboljšanja koja korisniku ostaju transparentna, može se spomenuti bolja zaštita korisnika od aktivnih skripti koje pokušavaju promijeniti veličinu prozora, ili promijeniti njegovu poziciju s ciljem zavaravanja korisnika.

9. Održavanje računala

Kako bi se korisniku olakšalo održavanje računala, sa Service Pack 2 zakrpom dolaze i dodatne funkcionalnosti vezane uz mogućnosti njegovog održavanja i nadzora. Osvježavanje sustava obavlja se automatski, zakrpe su manje, a za administraciju je predviđeno centralizirano sučelje po nazivom Security Center.

9.1. Osvježavanje Windows XP operacijskog sustava

Nakon prvog pokretanja sustava nakon instalacije Service Pack 2 zakrpe, pokreće se automatska provjera da li su raspoložive nove sigurnosne zakrpa koje na sustavu nisu primijenjene. Ukoliko je to slučaj obavlja se njihov prijenos i instalacija kako bi sustav bio u potpunosti osvježen sa zakrpama koje su objavljene nakon izdavanja Service Pack 2 paketa. Windows Update 5 je nova inačica programa za osvježavanje Windows XP operacijskog sustava.

Osvježavanje se obavlja vrlo jednostavno putem Internet Explorer Web preglednika. Nakon što se odabere način instalacije (samo kritične zakrpe ili pregled svih dostupnih zakrpa), obavlja se *online* provjera koje su zakrpe nužne za instalaciju s ciljem uklanjanja otkrivenih problema. Nakon prijenosa odabranih zakrpa instalacija se može obaviti odmah, ili se može odgoditi za kasnije. Moguće je i automatsko osvježivanje sustava u točno definirano vrijeme, što je pogodno za korisnike koji imaju stalnu vezu na Internet.

Slika 11: Automatsko osvježavanje sustava

9.2. Security Center

Security Center je centralizirano sučelje za pregled i kontrolu svih zadataka vezanih za sigurnost sustava. Ovdje je moguće pronaći tri glavne sigurnosne funkcije: Windows vatrozid, automatsko osvježavanje sustava i zaštita od malicioznih programa. Ukoliko Security Center uoči neki problem, vezan uz bilo koji od navedenih aspekata zaštite, korisnik se obavještava odgovarajućom porukom.

Preporuka koje postavke bi trebale biti kontinuirano aktivne su: automatsko osvježavanje sustava na dnevnoj bazi, aktivan vatrozid, te aktivan antivirusni program s najnovijom verzijom potpisa virusa. Status svakog elementa se također prikazuje unutar Security Centar sučelja (Slika 12).

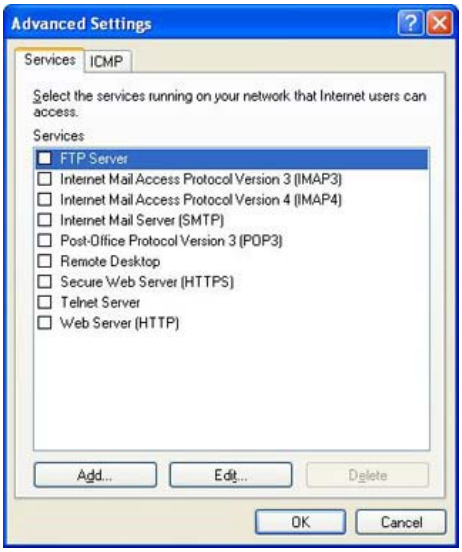
Slika 12: Security Center sučelje

10. Potencijalni problemi

Pojavom Service Pack 2 zakrpe pojavili su se i brojni problemi vezani uz kompatibilnost postojećih aplikacija s novim sigurnosnim politikama i izmjenama na operacijskom sustavu, kao što su onemogućeni Alerter i Messenger servisi, problemi vezani uz vatrozid, te nemogućnost izvođenja *backup-a* putem računalne mreže. Kako novi vatrozid provodi prilično strogu kontrolu dolaznog mrežnog prometa, mogući su problemi prilikom udaljene administracije, *peer-to-peer* spajanja, FTP ili Microsoft IIS konekcija. Problemi aplikacija se mogu klasificirati u dvije kategorije: oni koji nastaju jer programska podrška nije kompatibilna s SP 2 paketom, i oni koji nastaju zbog prisutnosti vatrozida. Prvi tip problema je daleko ozbiljniji, dok se drugi tip problema uspješno rješava promjenom konfiguracije vatrozida, i uglavnom se odnosi na otvaranje pojedinih portova i dodavanja aplikacija na listu iznimaka.

10.1. Web poslužitelji

Vatrozid je podešen da inicijalno blokira svaku aktivnost na većini mrežnih portova. Kako bi se omogućilo nesmetano pokretanje aplikacija, svi portovi koje aplikacija zahtjeva moraju biti identificirani i otvoreni. Ukoliko se npr. želi sustav konfigurirati tako da na njemu bude pokrenut Web poslužitelj, TCP port 80 mora biti otvoren za spajanje. Ova opcija se pojavljuje u naprednim postavkama sučelja vatrozida (Slika 9).



Slika 13: Lista servisa dostupnih sa Interneta

10.2. Sigurnosna pohrana podataka putem računalne mreže

Inicijalne postavke vatrozida neće dozvoliti provođenje *backup*-a putem računalne mreže. Izvršavanje udaljenog *backup*-a putem NetWorker, VERITAS i ARCServe aplikacija neće raditi jer ovim aplikacijama neće biti dozvoljeno spajanje na udaljeni sustav. Vrlo vjerojatno će se prijaviti greška "*Netwok path not found*". Kako bi se uklonio ovaj problem potrebno je navedene aplikacije dodati na listu iznimki vatrozida, čime će im se omogućiti legitiman pristup računalu.

10.3. Problemi s antivirusnim programima

Također su mogući i problemi sa antivirusnim programima. Ovdje spada nekoliko izdavača između kojih se nalaze i McAfee, SOURCENEXT, SonicWall i Command AntiVirus. Problemi se manifestiraju na različite načine, uključujući nemogućnost pokretanja programa i nasilno prekidanje rada sustava. Vjerojatnije da će do problema doći sa starijim inačicama softvera navedenih izdavača.

10.4. Nero programski paket

Nakon instalacije Service Pack 2 zakrpe, prilikom pokretanja Nero aplikacije javlja se upozorenje o problemu kompatibilnosti ovog programa s instaliranom inačicom sustava (Slika 14). Upozorenje sadrži i obavijest da je potrebno posjetiti Web stranice izdavača ove aplikacije s ciljem uklanjanja ovog problema. Iako se pojavljuje ovo upozorenje, nastavkom rada sve se odvija normalno, i osnovne operacije Nero aplikacije funkcioniraju ispravno i bez osvježavanja.

Slika 14: Prijava problema kod Nero aplikacije

10.5. Ostali problemi

Među ostalim problemima koji se javljaju nakon instalacije Service Pack 2 zakrpe treba ubrojiti probleme s Netzero softverom za povezivanje na Internet, probleme sa skenerima proizvođača UMAX, neispravno prikazivanje verzije USB upravljačkog programa i dr. Osim ovdje spomenutih problema postoji još mnogo njih koji se još uvijek sa sigurnošću ne mogu potvrditi. Mnogi korisnici prijavljuju razne probleme s kojima se susreću, međutim za većinu njih je vrlo vjerojatno da se pojavljuju upravo zbog neiskustva korisnika u radu s novom inačicom Windows XP operacijskog sustava, koja sada postavlja puno veća ograničenja od svojih prethodnih verzija.

11. Zaključak

Na temelju iznesenih informacija može se zaključiti da Windows XP Service Pack 2 donosi mnoga poboljšanja kojima se umanjuje rizik od prijetnji s Interneta. Promjene su vezane uz unaprjeđenu mrežnu zaštitu korištenjem Windows vatrozida, sigurnijom infrastrukturom distribuiranih COM komponenti, te promjenama na RPC servisima. Zaštita memorije osigurava se hardeverski na arhitekturama procesora koje to podržavaju, te softverski tamo gdje to nije moguće.
Korisnicima se pruža veća sigurnost i u obradama primljenih poruka, bilo putem e-mail ili *instant messaging* servisa. Poboljšanja su prisutna i kod Internet Explorer Web preglednika kako bi se osiguralo sigurnije pretraživanje sadržaja na Internetu. Kako je za sigurnost sustava vrlo važno redovito osvježavanje najnovijim sigurnosnim zakrpama, kroz Windows Update servis nudi se i mogućnost jednostavnog i automatskog osvježavanja, što korisnicima pomažu pri održavanju koraka s najnovijim sigurnosnim prijetnjama. Osim svega navedenog, administracija i upravljanje osnovnim sigurnosnim aspektima sustava je centralizirano kroz uvođenje novog sučelja, Security Centra.
No, osim brojnih poboljšanja i noviteta koje SP2 zakrpi donosi, primijećeni su i određeni problemi koji se prvenstveno javljaju kao posljedica nekompatibilnosti zakrpe sa pojedinim programskim paketima i aplikacijama. Iako je većina tih problema vezana uz neispravno podešavanje i korištenje novih funkcionalnosti XP SP2 zakrpe, postoje i ozbiljni problemi koji uzrokuju neočekivane probleme u radu sustava. Naravno, u ovom pogledu očekuje se odgovarajuća podrška od samog Microsfta, kako bi se svi ovi problemi pravovremeno uklonili i kako bi se korisnicima pružila odgovarajuća razina zaštite.

12. Reference

[1] Microsoft, Changes to Functionality in Microsoft Windows XP Service Pack 2,
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx
[2] Steve Friedl's Unixwiz.net Tech Tips, Analysis of Microsoft XP Service Pack 2,
http://www.unixwiz.net/techtips/xp-sp2.html
[3] Microsoft, Windows XP Service Pack 2 Overview White Paper,
http://msdn.microsoft.com/security/productinfo/xpsp2/default.aspx