HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sigurnost osobnih računala s Windows operacijskim sustavom

CCERT-PUBDOC-2005-07-129

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

Zaštita osobnih računala od neovlaštenog pristupa važna je radi ostvarivanja odgovarajuće razine zaštite korisničkih podataka. U odnosu na korporativna stolna računala koja su ipak pod nadzorom sistem administratora, i gdje se povjerljivi podaci pretežito pohranjuju na mrežnim poslužiteljima, prijenosna i kućna računala vrlo su često znatno slabije zaštićena. Kod prijenosnih računala dodatni problem predstavlja mogućnost njihovog gubitka ili krađe, što potencijalnom napadaču otvara dodatne mogućnosti kompromitiranja sustava. Također, današnje performanse i kapaciteti prijenosnih računala korisnicima omogućuju nesmetano obavljanje poslovnih podataka sa različitih lokacija (od kuće, iz hotelskih soba, konferencijskih dvorana i sl.), tako da se sve češće na njima mogu pronaći brojne povjerljive privatne i poslovne informacije. Kompromitiranje računala u tom slučaju predstavlja iznimno visoki sigurnosni rizik te je potrebno poduzeti sve preventivne sigurnosne mjere kako bi se to onemogućilo.
Dokument opisuje osnovne postupke kojima je razinu sigurnosti stolnih i prijenosnih računala s Windows operacijskim sustavom moguće podići na višu razinu. Analizirani su osnovni problemi koji se javljaju u ovom pogledu te mogućnosti njihovog uklanjanja.

2. Sigurnost na razini operacijskog sustava

Sigurnost Microsoft Windows operacijskih sustava oduvijek je bila tema o kojoj se mnogo raspravljalo. Naime, dobro je poznato da se različite inačice Windows operacijskih sustava razlikuju po svojim sigurnosnim karakteristikama, i da su neke od njih danas potpuno neprihvatljive sa stanovišta sigurnosti. Inačice koje se danas nikako ne preporučuje instalirati na osobna računala su Windows 95, Windows 98 i Windows ME sustavi koji su poznati po brojnim sigurnosnim nedostatcima, što možda i nije toliko iznenađujuće budući da se sigurnost u vrijeme njihovog nastajanja mnogo drugačije tretirala nego što je to danas slučaj. U trenutku pisanja ovog dokumenta preporučljive inačice Windows sustava za osobna računala su Windows 2000 Professional te Windows XP Professional sustavi sa odgovarajućim sigurnosnim zakrpama (SP4 za W2K sustave te SP2 za WinXP sustave).

2.1. Instalacija operacijskog sustava i dodatnih komponenti

Prilikom kupovine računala korisnici trebaju inzistirati na Windows 2000 ili XP Professional inačici operacijskog sustava, kao što je već ranije spomenuto. U odnosu na Windows XP Home Edition, koja je uobičajena inačica koju dobavljači isporučuju s osobnim računalima, preporučene inačice sadrže određena svojstva koja ih čini mnogo prihvatljivijima sa stanovišta sigurnosti. Windows XP Home Edition sustav namijenjen je manje iskusnim korisnicima te su stoga i mnoge postavke sustava u tom smjeru prilagođene.
Neke od značajnijih karakteristika koje su prisutne kod Win XP Professional sustava, a ne postoje kod Home Edition inačice su:

- Encrypting File System,
- Automated System Recovery (ASR),
- Remote Desktop,
- File-level access control,
- C2 razina sigurnosti.

Detaljnije informacije o razlikama između Windows XP Professional i Home Edition sustava moguće je pronaći na adresi http://www.winsupersite.com/showcase/windowsxp_home_pro.asp.
Nakon odabira i inicijalne instalacije operacijskog sustava, vrlo je važno da se prije povezivanja na računalnu mrežu primjene sve relevantne sigurnosne zakrpe. Njihovom instalacijom ukloniti će se svi dotad objavljeni sigurnosni nedostatci te će se sustav u određenoj mjeri zaštititi od neovlaštenih aktivnosti. Također, sa sigurnosnim zakrpama vrlo često dolaze i različite nadogradnje koje dodatno mogu podići razinu sigurnosti sustava.
Također, prije instalacije sigurnosnih zakrpi uvijek je preporučljivo napraviti sigurnosnu kopiju podataka s računala, kako bi se izbjegli eventualni problemi. Dodatno, tijekom instalacije zakrpe preporučljivo je odabrati opciju **Archive files** koja će omogućiti deinstalaciju sigurnosne zakrpe,

ukoliko se nakon instalacije pojave problemi u radu operacijskog sustava, programskih alata ili sklopovlja.
Ukoliko se želi provjeriti koja je trenutna inačica operacijskog sustava instalirana na računalu te da li je instalirana odgovarajuća sigurnosna zakrpa, potrebno je učiniti slijedeće:

1. kliknuti dugme `Start` te naredbu `Run`,
2. u polje `Open` upisati naredbu `winver`,
3. kliknuti dugme `OK`.

Slika 1 prikazuje informacije o inačici operacijskog sustava koji je instaliran na računalu.

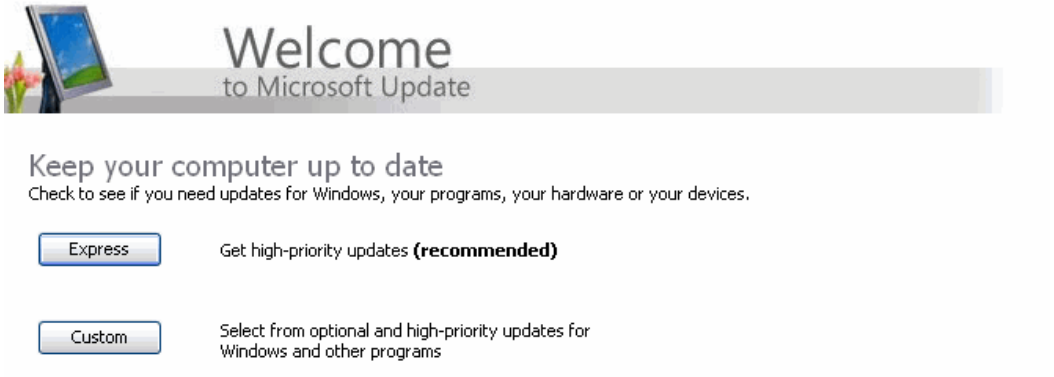
Slika 1: Informacija o inačici operacijskog sustava

2.2. Ažuriranje operacijskog sustava

Nakon instalacije operacijskog sustava i svih sigurnosnih zakrpi, potrebno je daljnje redovno ažuriranje operacijskog sustava. Razlog tomu jest svakodnevno pojavljivanje novih malicioznih programa te ranjivosti unutar operacijskog sustava i programskih paketa, koje mogu ozbiljno ugroziti sigurnost sustava. Microsoft redovito izdaje sigurnosne zakrpe za svoje proizvode koje uklanjaju novo uočene ranjivosti te ih je potrebno redovito primjenjivati kako bi se na sustavu održala zadovoljavajuća razina sigurnosti. Za ažuriranje operacijskog sustava koristi se *Windows Update* servis unutar Windows operacijskog sustava. Moguće je koristiti manualno i automatsko ažuriranje.
Manualno ažuriranje izvodi se prema slijedećim koracima:

1. računalo spojiti na Internet,
2. u Internet pretraživaču otvoriti adresu http://windowsupdate.microsoft.com, ili
3. odabrati naredbu `Windows Update` iz izbornika `Start` koja otvara stranicu navedenu pod točkom 2.,
4. odabrati način instalacije,

   Po otvaranju *Windows Update* web stranice otvara se stranica prikazana na slici Slika 2 u kojoj korisnik bira način na koji će izvršiti ažuriranje.

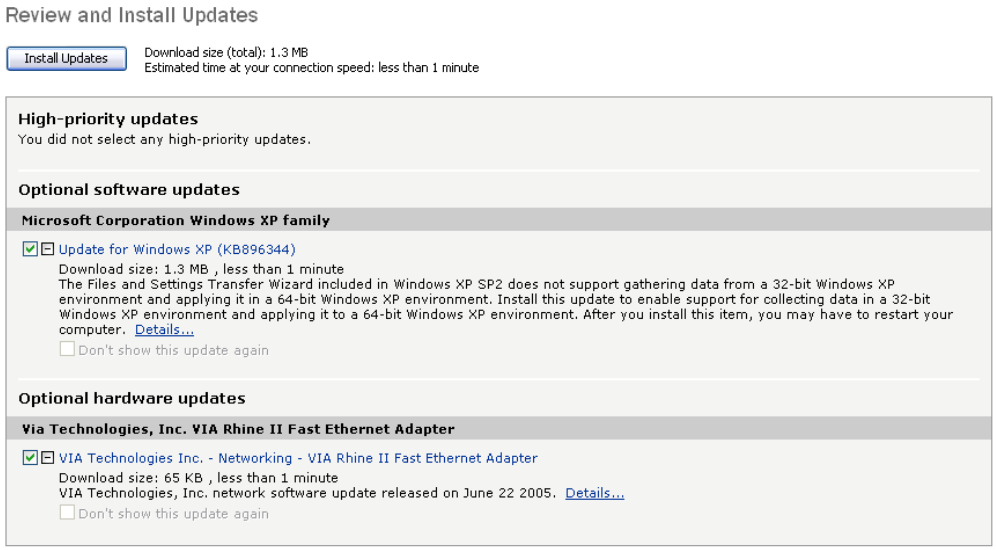


Slika 2: Izbor načina ažuriranja operacijskog sustava

Express način instalacije omogućuje da se instaliraju zakrpe visokog prioriteta (engl. *high priority*) što je preporučljivo za manje iskusne korisnike. Ovim načinom korisnik treba

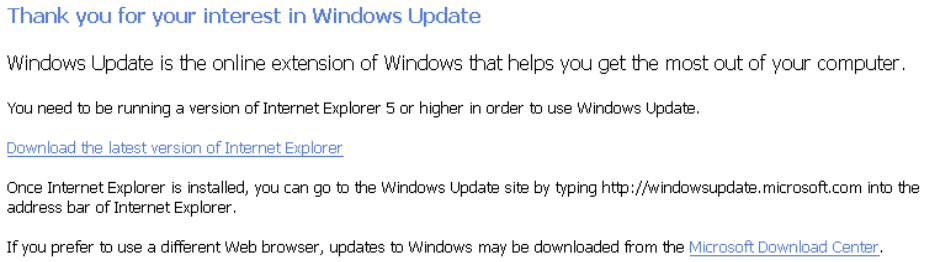
potvrditi instalaciju te pričekati da proces instalacije završi. *Custom* način instalacije korisniku omogućuje izbor između opcionalnih zakrpa za programske alate i sklopovlje te zakrpa visokog prioriteta. Ovaj način ažuriranja preporučljiv je za iskusnije korisnike jer se pojedinačno biraju zakrpe koje se žele instalirati na računalo.

5. potvrditi instalaciju odabranih stavki klikom na dugme `Install Updates`,
   Slika 3 prikazuje stranicu nakon što su korisnički odabrane stavke za instalaciju. Po izboru stavki potrebno je potvrditi instalaciju.



Slika 3: Korisnički odabrane opcije za ažuriranje

6. pričekati završetak procesa instalacije,
   Ukoliko korisnik upotrebljava neki drugi Internet pretraživač, a ne *Microsoft Internet Explorer*, dobit će informaciju o tome da može instalirati najnoviju inačicu *Internet Explorer* pretraživača ili može otvoriti *Microsoft Download Center*, Web stranicu na kojoj će birati proizvod koji želi ažurirati, a koja se nalazi na lokaciji http://www.microsoft.com/downloads/search.aspx?displaylang=en. Informativna stranica prikazana je na slici Slika 4.



Slika 4: Informativna stranica

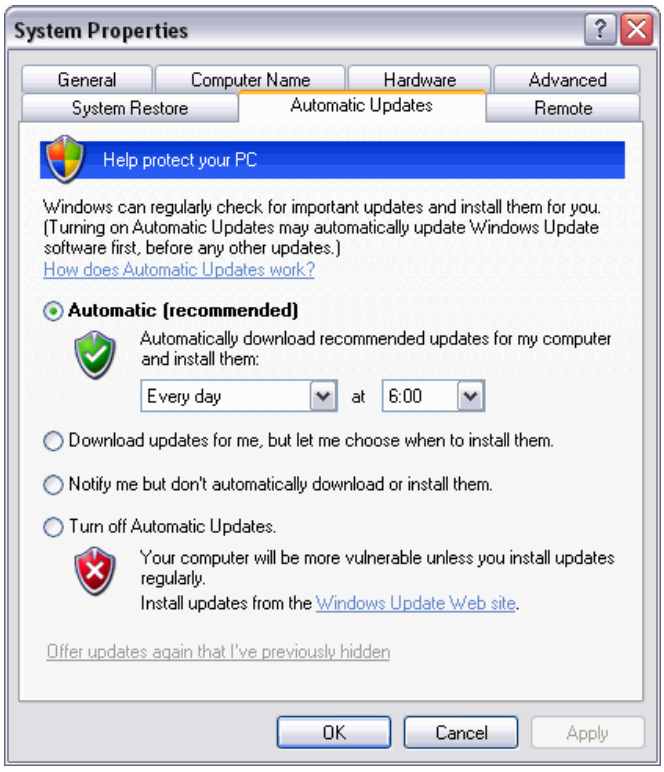
7. ponovno pokrenuti operacijski sustav.
   Nakon instalacije zakrpi, operacijski sustav potrebno je ponovno pokrenuti kako bi se primijenile ažurirane promjene. Sve dok se operacijski sustav ponovno ne pokrene, nije moguće dalje koristiti *Windows Update* svojstvo tj. onemogućeno je daljnje ažuriranje operacijskog sustava.

Za korištenje automatskog načina ažuriranja operacijskog sustava poželjno je imati stalnu vezu na Internet, u protivnom će se automatsko ažuriranje provoditi samo onda kada je računalo spojeno na Internet. Podešavanje postavki za ovakav način ažuriranja operacijskog sustava izvodi se prema slijedećim koracima:

1. desnom tipkom miša kliknuti na ikonu `My Computer` i odabrati naredbu `Properties`,

2. odabrati karticu `Automatic Updates`,
3. odabrati opciju `Automatic (recommended)`,
4. kliknuti dugme OK.

Slika 5 prikazuje dijaloški okvir automatskog ažuriranja operacijskog sustava.



Slika 5: Podešavanje automatskog ažuriranja operacijskog sustava

2.3. Uporaba NTFS datotečnog sustava

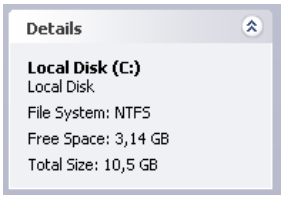
Na Windows operacijskim sustavima postoje dva tipa datotečnih sustava: FAT/FAT32 (*File Allocation Table*) i NTFS (*NT File System*) datotečni sustav. Od pojave Windows NT operacijskog sustava, kada se pojavio NTFS datotečni sustav, preporuka je da se koristi uglavnom navedeni datotečni sustav jer omogućava višu razinu sigurnosti datoteka i mapa na računalima. Izbor datotečnog sustava računala provodi se prilikom instalacije operacijskog sustava kada korisnik bira hoće li se lokalni disk formatirati u FAT/FAT32 ili NTFS datotečnom sustavu.

Međutim, ako je prilikom instalacije odabran FAT/FAT32 datotečni sustav, on se može pretvoriti u NTFS sustav bez brisanja svih podataka s računala upotrebom `convert` naredbe.

Ukoliko je operacijski sustav već instaliran na računalu, korisnik može provjeriti koji je datotečni sustav izabran prilikom instalacije na slijedeći način:

1. otvoriti ikonu `My Computer`,
2. kliknuti na lokalni disk `x:` gdje `x` predstavlja slovo lokalnog diska za koji se želi provjeriti datotečni sustav,
3. u lijevom dijelu prozora My Copmuter pogledati polje `Details` koje sadrži informaciju `File System`.

Informacije o datotečnom sustavu odabranog lokalnog diska prikazane su na slici Slika 6.

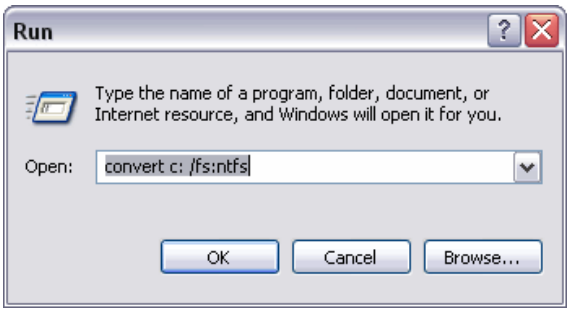


Slika 6: Informacija o datotečnom sustavu

Pretvorba FAT/FAT32 datotečnog sustava u NTFS datotečni sustav izvodi se prema slijedećim koracima:

1. napraviti kopiju svih podataka koji se nalaze na računalu,
2. kliknuti dugme `Start` te naredbu `Run`,
3. upisati naredbu `convert x: /fs:ntfs` pri čemu je `x` slovo lokalnog diska čiji se datotečni sustav pretvara iz jednog oblika u drugi,
4. kliknuti dugme `OK`,
5. pričekati završetak procesa pretvorbe,
6. ponovno pokrenuti operacijski sustav.

Slika 7 prikazuje dijaloški okvir naredbe `Run` nakon upisa naredbe za pretvorbu (točka 3 ove liste koraka).



Slika 7: Upotreba naredbe `convert`

2.4. Zaštita podataka enkripcijom

EFS (engl. *Encrypted File System*) je sigurnosno svojstvo NTFS datotečnog sustava Windows 2000 i XP Professional operacijskih sustava. Omogućuje zaštitu podataka enkripcijom na razini datoteka i na razini mapa. Ukoliko se EFS primjeni nad određenom mapom, sve datoteke unutar te mape biti će zaštićene. Nakon što se primjeni EFS nad mapom ili datotekom, pristup istoj će biti omogućen samo autoriziranom korisniku. Svi ostali korisnici neće biti u mogućnosti pristupiti enkripcijom zaštićenim podacima.

Enkriptiranje podataka upotrebom *Windows EFS* sustava izvodi se na slijedeći način:

1. desnom tipkom miša kliknuti datoteku ili mapu koja se želi zaštititi i odabrati naredbu `Properties`,
2. na kartici General kliknuti dugme `Advanced`,
3. označiti opciju `Encrypt contents to secure data` (Slika 8),
4. kliknuti dugme `OK` na prozoru `Advanced Attributes`,
5. kliknuti dugme `OK` na prozoru `Private Properties`,
6. ukoliko se štiti mapa, odabrati opciju `Apply changes to this folder, subfolder and files` kako bi se sve unutar odabrane mape zaštitilo enkripcijom (Slika 9),
7. pričekati kraj procesa.

Slika 8: Uključivanje opcije za enkripciju podataka

Slika 9: Primjena enkripcije na sav sadržaj unutar odabrane mape

Bitna napomena prilikom korištenja EFS sustava jest da se ona preporučuje samo za ona računala koja su u Windows domeni. Naime, ukoliko korisnik čije računalo nije u domeni upotrijebi ovu mogućnost zaštite podataka, u slučaju pada operacijskog sustava nije moguće povratiti enkriptirane podatke. Ukoliko je računalo u Windows domeni tada je moguće upotrebom *recovery agent* korisničkog računa i certifikata povratiti podatke s lokalnog diska. Ono što korisnik računala koje nije u Windows domeni mora odlučiti, prije upotrebe ove mogućnosti, jest da li su podaci koje ima na računalu toliko osjetljivi da je manja šteta izgubiti ih nepovratno nego li mogućnost da ih vidi neovlaštena osoba.

2.5. Podešavanje postavki Internet Explorer pretraživača

Podešavanje postavki Internet Explorer Web preglednika poželjno je provesti za sve korisnike koji upotrebljavaju ovaj pretraživač za pregledavanje stranica na Internetu.
Naime, razlog zbog kojeg se ova sigurnosna mogućnost izdvaja kao bitna jest to što određene Web stranice sadrže nesigurne skripte i ActiveX kontrole. Prilikom posjete takvih stranica, skripte se automatski dohvaćaju sa stranice i izvršavaju unutar pretraživača. Takva vrsta skripti uglavnom ima maliciozno djelovanje na računalu pa se stoga preporučuje korisnicima podešavanje Internet Explorer pretraživača prema slijedećoj tablici:

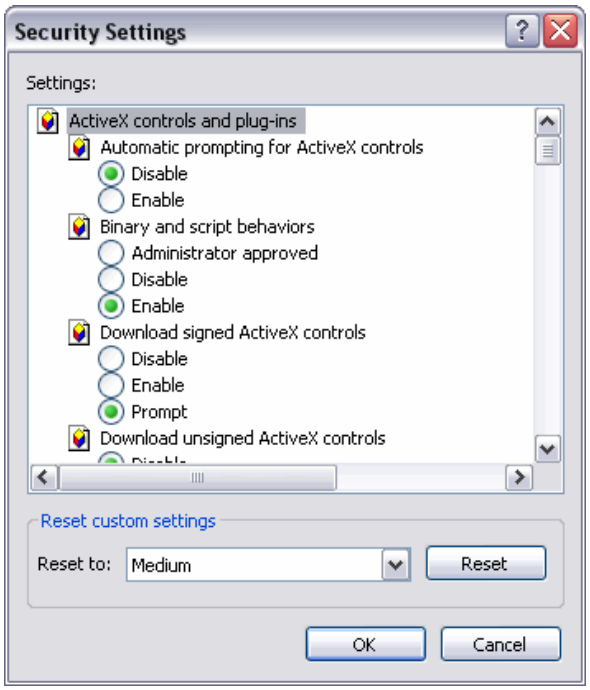
Sekcija	Postavke	Akcija
ActiveX controls and plug-ins	Download signed ActiveX Controls	Prompt
	Download unsigned ActiveX Controls	Disable
	Initialize and script ActiveX Controls not marked as safe	Disable
Scripting	Allow paste operations via script	Prompt

Sekcija	Postavke	Akcija
Java	Java permissions	High safety
Miscellaneous	Access to dana sources across domains	Disable

Tablica 1: Postavke Internet Explorera

Postavke se podešavaju na slijedeći način:

1. otvoriti `Internet Explorer`,
2. u izborniku `Tools` odabrati naredbu `Internet Options`,
3. na kartici `Security` kliknuti dugme `Custom Level`,
   Otvara se dijaloški okvir `Security Settings` prikazan na slici Slika 10 u kojem korisnik podešava postavke kako je navedeno u tablici Tablica 1.



Slika 10: Podešavanje postavki u Internet Explorer-u

4. kliknuti dugme OK unutar prozora `Security Setings`,
5. kliknuti dugme OK unutar prozora `Internet Options`.

2.6. Onemogućavanje nepotrebnih servisa

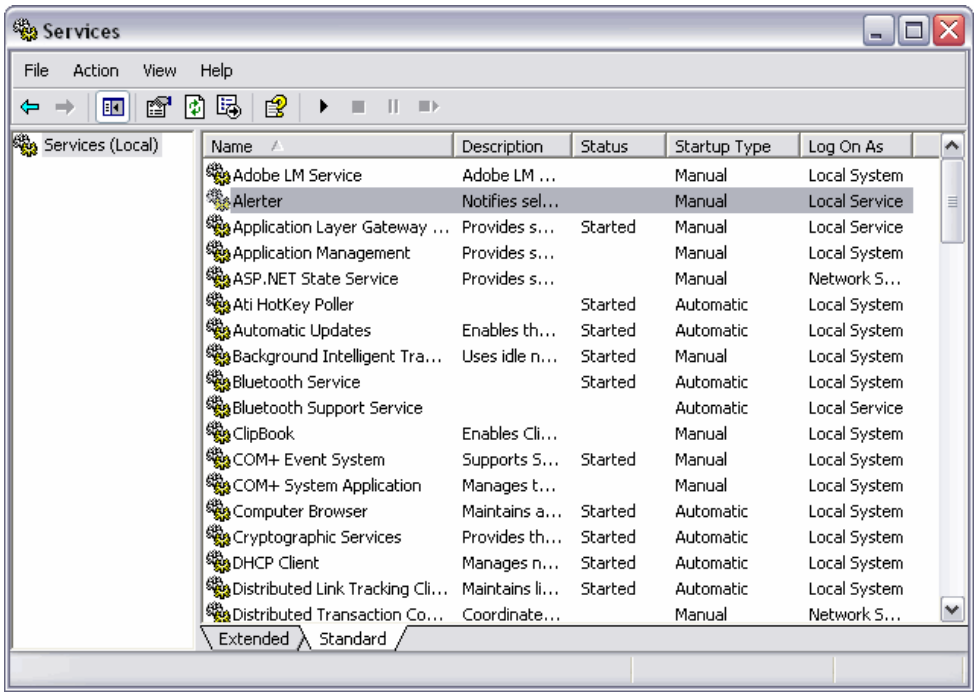
Operacijski sustav ima mnoštvo aktivnih servisa koji su predefinirani procesom instalacije, pa je preporučljivo onemogućavanje onih servisa koji su nepotrebni tj. koje korisnik ne upotrebljava. Ranjivosti servisa koji nisu potrebni korisniku mogu se iskoristiti za neovlašteni pristup računalu. Njihovim onemogućavanjem smanjuje se mogućnost napada, a ujedno se povećavaju i performanse računala. Slijedeći servisi mogu se onemogućiti i Windows operacijski sustavi će nastaviti funkcionirati neometano:

```
Alerter
Application Management
Clipbook
Distributed Link Trakcing Client
Distributed Transaction Coordinator
Human Interface Device Access / HID Input Service
IIS Admin
Indexing Service
Messanger
```

```
NetMeeting Remote Desktop Sharing
Network DDE
Network DDE DSDM
Network Provisioning Service
QoS RSVP
Remote Registry
Routing and Remote Access
Telnet
Windows Management Instrumentation Driver Extensions
WMI Performance Adapter
```

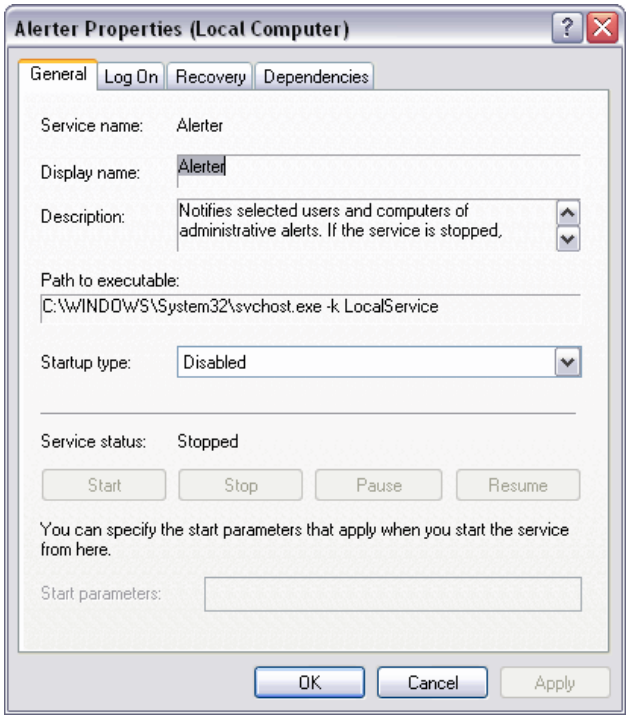
Za onemogućavanje navedenih servisa ili onih koje korisnik ne upotrebljava, a bez utjecaja na funkcionalnost rada operacijskog sustava, treba učiniti slijedeće:

1. kliknuti dugme `Start` i odabrati naredbu `Run`,
2. u polje `Open` upisati `services.msc`,
3. kliknuti dugme `OK`,
   Otvara se konzola `Services` u kojoj je popis svih servisa operacijskog sustava, koji je prikazan na slici Slika 11.



Slika 11: Popis servisa

4. dvostruko kliknuti servis iz prethodnog popisa pri čemu se otvara dijaloški okvir `ime_servisa Properties (Local Computer)` prikazan na slici Slika 12.



Slika 12: Svojstva servisa

5. na kartici `General`, u polju `Service status` provjeriti da je servis zaustavljen, a u slučaju da nije, kliknuti dugme `Stop`,
6. na kartici `General`, u polju `Startup type` odabrati `Disabled` opciju,
7. kliknuti dugme `OK`.

Otvaranjem dijaloškog okvira prikazanog na slici (Slika 12) korisnik može vidjeti opis servisa te na taj način od navedenih servisa onemogućiti zaista one koje ne upotrebljava.

2.7. Optimizacija sigurnosnih postavki

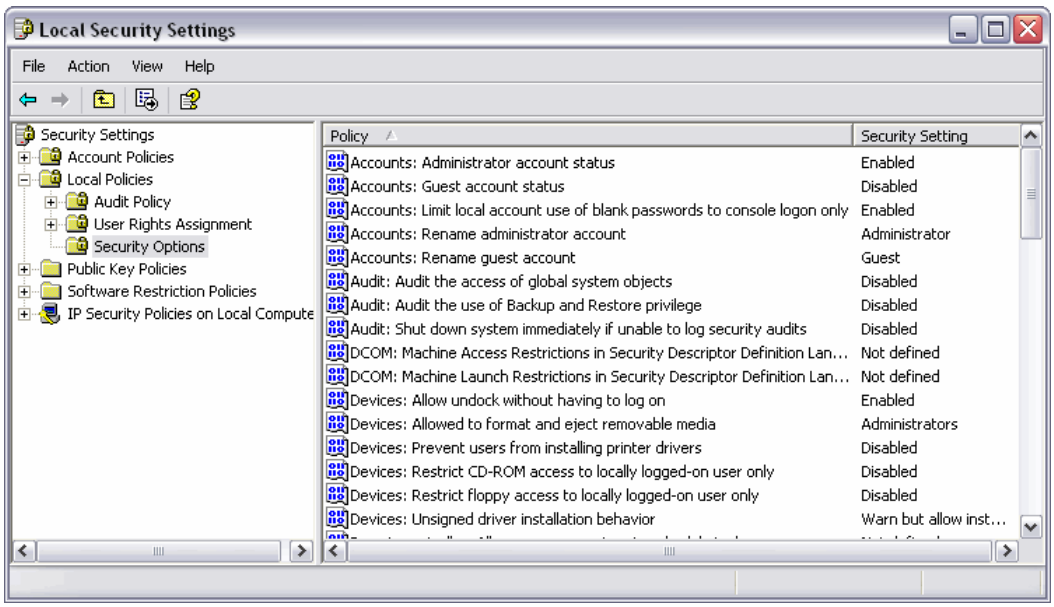
Predefinirana instalacija Windows operacijskog sustava sadrži određene nesigurne postavke koje ostavljaju otvorenom mogućnost napada na računalo. Preporučuje se podešavanje postavki kao što je navedeno u tablici Tablica 2, ne bi li se smanjio rizik od neovlaštenog pristupa računalu:

Windows XP Professional Security Option Policy	Preporučena postavka
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
Devices: Restrict floppy access to locally logged-on user only	Disabled
Interactive logon: Do not display last user name	Disabled
Interactive logon: Do not require CTRL+ALT+DELETE	Disabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allows anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Do not allow storage of credentials of .NET Passports for network authentication	Enabled
Network access: Named Pipes that can be accessed anonymously	Izbrisati sve zapise
Network access: Remotly accessible registry paths	Izbrisati sve zapise

Tablica 2: Postavke sigurnosnih politika

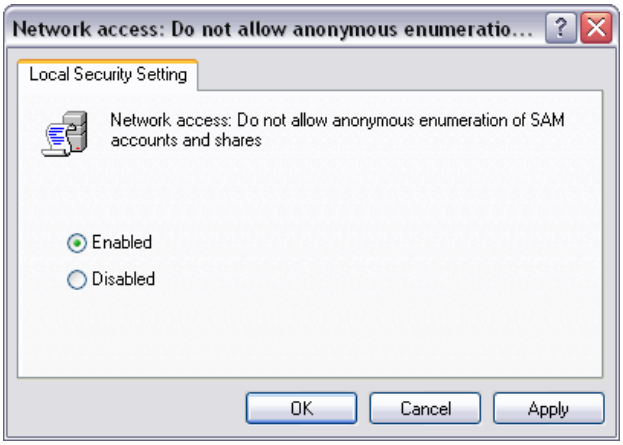
Navedene postavke podešavaju se na slijedeći način:

1. kliknuti dumge `Start` i odabrati naredbu `Run`,
2. u polje `Open` upisati naredbu `secpol.msc`,
3. kliknuti dugme `OK`,
   Otvara se prozor `Local Security Settings` prikazan na slici Slika 13.



Slika 13: Sigurnosne politike

4. u prozoru kliknuti na `Security Settings`, `Local Policies`, `Security Options`,
5. u desnom dijelu prozora dvostruko kliknuti na politike navedene u tablici pri čemu se otvara prozor svojstava odabrane politike prikazan na slici Slika 14,



Slika 14: Svojstva politike

6. odabrati postavku koja je preporučena u tablici,
7. kliknuti dugme `OK`.

2.8. Podešavanje politike korisničkih računa

Osim optimizacije sigurnosnih postavki putem sigurnosnih politika, potrebno je povećati sigurnost i podešavanjem politike korisničkih računa. Podešavanje korisničkih računa odnosi se na podešavanje politike zaporki i politike zaključavanja korisničkog računa.

Preporučljive postavke za politiku zaporki prikazane su u tablici Tablica 3, a za zaključavanje korisničkog računa u tablici Tablica 4.

Password Policy	Preporučena postavka
Enforce password history	5 password remembered
Maximum password age	30 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity reguirements	Enabled
Store password using reversible encryption	Disabled

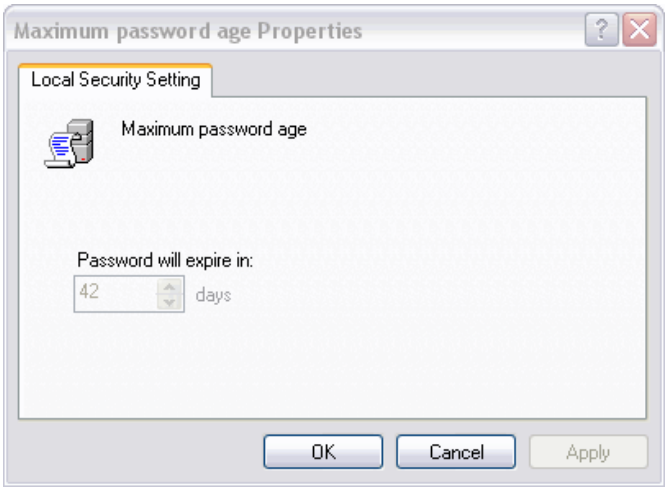
Tablica 3: Postavke politike zaporki

Account Lockout Policy	Preporučena postavka
Account lockout duration	30 minutes
Account lockout treshhold	5 invalid login attempts
Reset account lockout counter after	30 minutes

Tablica 4: Postavke politike zaključavanja korisničkog računa

Navedene postavke podešavaju se na slijedeći način:

1. kliknuti dumge `Start` i odabrati naredbu `Run`,
2. u polje `Open` upisati naredbu `secpol.msc`,
3. kliknuti dugme `OK`,
   Otvara se prozor `Local Security Settings` prikazan na slici Slika 13.
4. u prozoru kliknuti na `Security Settings`, `Account Policies`, `Password Policy`,
5. u desnom dijelu prozora dvostruko kliknuti na politike navedene u tablici pri čemu se otvara prozor svojstava odabrane politike prikazan na slici Slika 15,



Slika 15: Svojstva politike

6. podesiti postavku koja je preporučena u tablici,
7. kliknuti dugme `OK`,
8. u prozoru kliknuti na `Security Settings`, `Account Policies`, `Account Lockout Policy`,
9. u desnom dijelu prozora dvostruko kliknuti na politike navedene u tablici,
10. podesiti postavku koja je preporučena u tablici,
11. kliknuti dugme `OK`.

2.9. Dijeljenje resursa računala

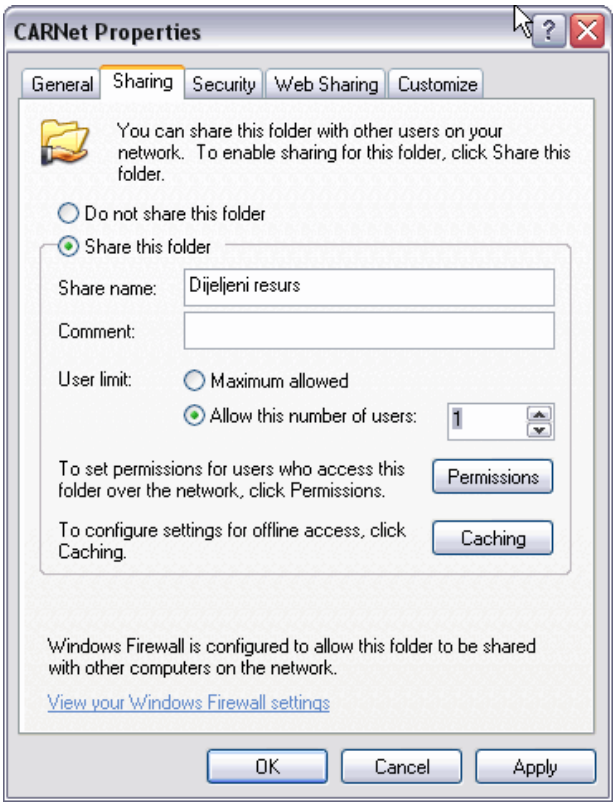
Prilikom definiranja dijeljenih resursa računala potrebno je definirati i njihove dozvole pristupa, što se često u praksi zaboravlja. Prilikom izbora resursa za dijeljenje za računala u domeni, treba se držati preporuka:

- dijeliti samo one resurse za koje postoji opravdana potreba dijeljenja,
- ograničiti pristup dijeljenim resursima na samo jednog korisnika istovremeno,
- podesiti pravila pristupa tako da se dodaju samo oni korisnički računi koji će koristiti dijeljene resurse, a obrisati grupu `Everyone`,
- dijeljenim resursima dati samo pravo `Read`, te izbjegavati pravo `Write` i `Full control`,
- provoditi redovitu provjeru dijeljenih resursa.

Za dijeljenje resursa i podešavanje sigurnosnih postavki istih treba učiniti slijedeće:

1. desnom tipkom miša kliknuti na resurs (disk, mapu, pisač) koji se želi dijeliti,
2. odabrati opciju `Sharing and Security`,
3. označiti opciju `Share this folder`,
4. u polju `User limit` odabrati opciju `Allow this number of users` i podesiti vrijednost na `1`,
5. kliknuti dugme `Permissions`,
6. kliknuti na grupu `Everyone` te na dugme `Remove` kako bi se izbrisala odabrana grupa,
7. klikom na dugme `Add` dodati one korisničke račune kojima se dopušta pristup dijeljenom resursu,
8. korisničkim računima omogućiti samo `Read` pravo,
9. kliknuti dugme `OK`.

Slika 16 prikazuje dijaloški okvir u kojem se određuju svojstva dijeljenog resursa.

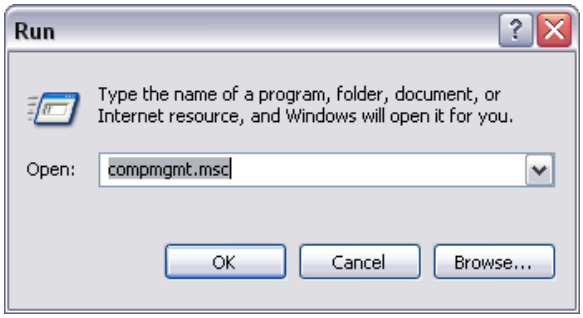


Slika 16: Podešavanje dijeljenog resursa

Kako bi korisnik pregledao sve dijeljene resurse na svom računalu treba slijediti korake:

4. kliknuti dugme `Start` te naredbu `Run`,
5. u polje `Open` upisati naredbu `compmgmt.msc`,
6. kliknuti dugme `OK`

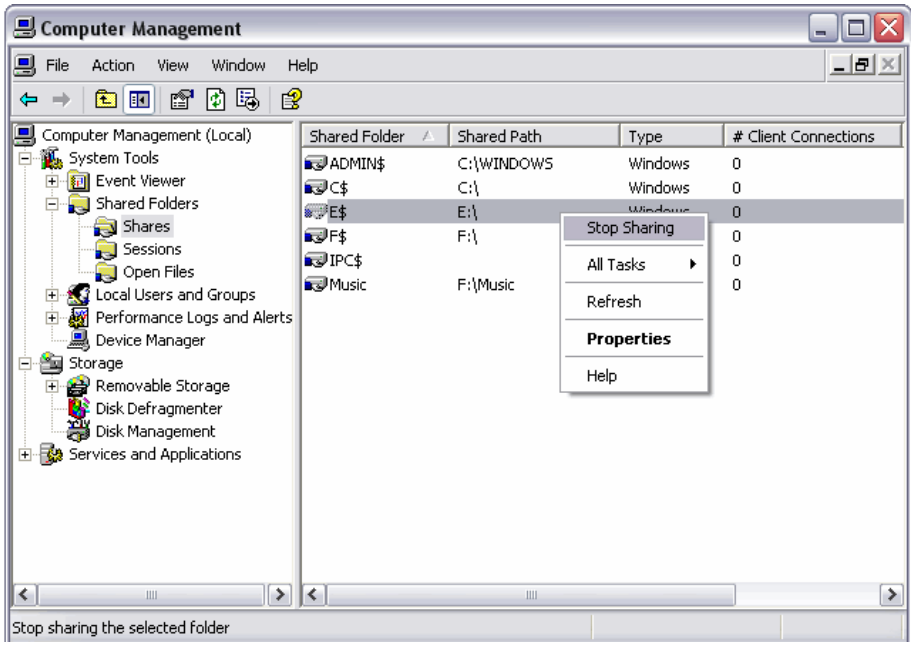
   Slika 17 prikazuje dijaloški okvir naredbe `Run` nakon upisa naredbe za otvaranje konzole i pregled dijeljenih resursa (točka 2 ove liste koraka).



Slika 17: Podešavanje dijeljenog resursa

   Otvara se prozor `Computer Management` prikazan na slici Slika 18.
7. u prozoru kliknuti na `System Tools`, `Shared Folders`, `Shares`,
8. u desnom dijelu prozora prikazan je popis svih dijeljenih resursa.

   Ukoliko korisnik želi zaustaviti dijeljenje nekog od navedenih resursa potrebno je:
   a. kliknuti desnom tipkom miša na željeni resurs,
   b. odabrati naredbu `Stop Sharing` kao što je prikazano na slici Slika 18,
   c. na upozorenje o prestanku dijeljenja resursa odgovoriti s `Yes`,



Slika 18: Podešavanje dijeljenog resursa

3. Dodatni sigurnosni alati

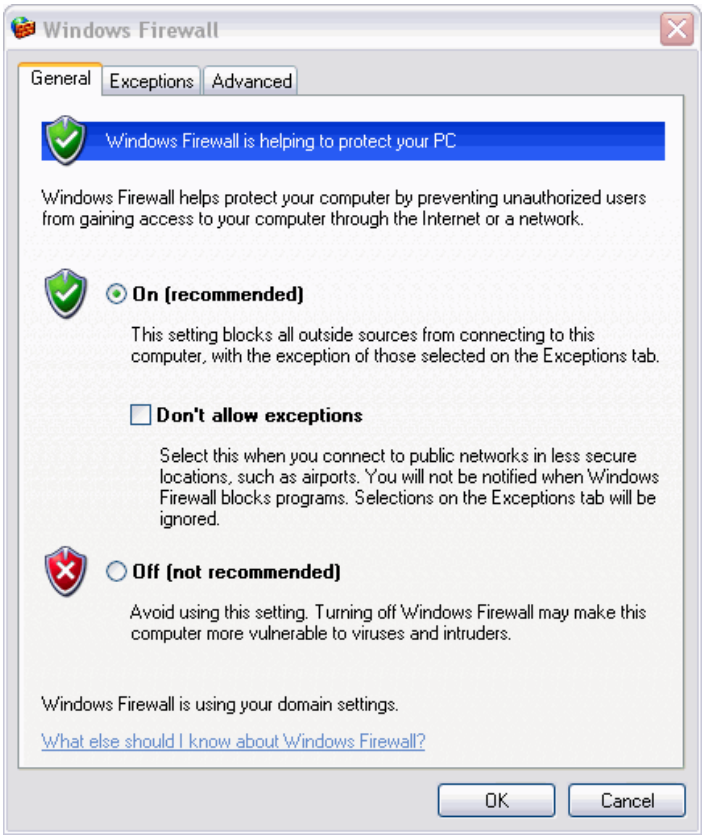
Osim podešavanja sigurnosnih postavki samog operacijskog sustava, sigurnost računala može se podići na višu razinu i upotrebnom programskih alata kao što su osobni vatrozid, antivirusni programski alat te antispyware programski alat.

3.1. Osobni vatrozid

Za zaštitu osobnih računala od neovlaštenih aktivnosti koriste se različiti mehanizmi, a jedan od njih je i osobni vatrozid. Vatrozid računalo u određenoj mjeri štiti od malicioznih aktivnosti s javnog Interneta i posebnu važnost ima kod računala koja koriste stalnu vezu na Internet. Podešavanjem sigurnosne politike vatrozida moguće je definirati koji je mrežni promet dozvoljen, a koji ne, što u velikoj mjeri doprinosi podizanju razine sigurnosti. Naravno, kao i sve druge sigurnosne kontrole, vatrozid ne pruža 100% zaštitu od malicioznih aktivnosti, već samo predstavlja jedan segment zaštite računala.

Windows XP Professional inačica operacijskog sustava s XP SP2 zakrpom dolazi sa ugrađenim osobnim vatrozidom. Njegovo podešavanje izvodi se na slijedeći način:

1. kliknuti dugme `Start` te naredbu `Control Panel`,
2. u prozoru dvostruko kliknuti ikonu *Windows Firewall*.
3. u prozoru *Windows Firewall* koji je prikazan na slici Slika 19 odabrati opciju `On (recommended)`.



Slika 19: Podešavanje vatrozida

Prozor se sastoji od tri kartice. Prva kartica `General` omogućava uključivanje (`On (recommended)`) odnosno isključivanje (`Off (not recommended)`) korištenja vatrozida. Na kartici `Exeptions` dodaju se programi, servisi i portovi kojima je dozvoljen promet mrežom. Kartica `Advanced` sadrži napredne opcije podešavanja Windows vatrozida.

Ukoliko korisnik ne želi koristiti ugrađeni Windows vatrozid, preporučuje se izbor nekog od alata koji su dostupni na Web stranicama CARNet CERT-a (http://www.cert.hr/tools.php?kw=&lang=hr&os=&cat=10).

3.2. Antivirusni programski alat

Antivirusni programski alat ima za cilj štititi računalo od računalnih virusa, crva te ostalih malicioznih programa. Alat ove namjene kontinuirano pregledava računalo i detektira viruse te provodi akcije koje su definirane od strane korisnika.
Windows operacijski sustavi ne dolaze s uključenim antivirusnim programom, već je potrebno odabrati neki od besplatnih ili komercijalnih rješenja koja se nude na tržištu.
Neki od antivirusnih programskih alata ukratko su opisani i mogu se također dohvatiti s Web stranica CARNet CERT-a (http://www.cert.hr/tools.php?kw=&lang=hr&os=&cat=8).
Preporuke koje se mogu dati generalno, bez obzira koji se od alata koristi, su slijedeće:

1. dohvatiti s Internet stranice (ili naručiti) antivirusni programski alat,
2. instalirati ga prema uputama dobavljača,
3. ažurirati bazu potpisa antivirusnog programskog alata,
4. podesiti postavke korištenjem pomoći programskog alata:
    a. akcije prilikom detekcije virusa,
    b. automatsko ažuriranje baze potpisa virusa,
    c. automatsko pregledavanje računala na mjesečnoj bazi,
    d. pregledavanje prilikom pristupanja datoteci,
    e. pregledavanje poruka elektroničke pošte.

3.3. Antispyware programski alat

Spyware programi detaljno su opisani u dokumentima koji se mogu dohvatiti na adresama http://www.cert.hr/filehandler.php?did=194, http://www.cert.hr/filehandler.php?did=45 i http://www.cert.hr/filehandler.php?did=110 pa se u ovom dokumentu neće detaljnije obrađivati. Kao i kod antivirusnog programskog alata, niti antispyware program nije implementiran unutar Windows operacijskog sustava. Popis i opis nekih od poznatijih antispyware programa moguće je pronaći na Web stranicama CARNet CERT-a http://www.cert.hr/tools.php?kw=&lang=hr&os=&cat=9.
Generalne preporuke za korištenje antispyware programa, bez obzira koji se od alata koristi su:

1. dohvatiti s Internet stranice (ili naručiti) antispyware programski alat,
2. instalirati ga prema uputama dobavljača,
3. ažurirati antispyware programski alat,
4. podesiti postavke korištenjem pomoći programskog alata.

4. Fizička sigurnost prijenosnog računala

Za razliku od stolnih računala, prijenosa računala su pod povećanim rizikom od krađe pa je potrebno istaknuti važnost podizanja fizičke razine sigurnosti takvih računala.
Fizička sigurnost prijenosnog računala svodi se na dva jednostavna pravila:

1. poduzeti sve mjere kako prijenosno računalo ne bi bilo ukradeno,
2. ako je prijenosno računalo ukradeno, onemogućiti pristup podacima koji se nalaze na njemu.

Da bi se prijenosno računalo zaštitilo od krađe preporučljivo je koristiti kabel za zaključavanje prijenosnog računala (engl. *laptop cable lock*). Neki od proizvoda ove i slične namjene mogu se pogledati na web adresi http://www.targus.com/uk/accessories_security.asp no bitno je napomenuti kako je proizvode potrebno kupiti.
Pristup podacima na prijenosnom računalu treba biti zaštićen pristupnom zaporkom koja korištenje prijenosnih računala omogućava samo ovlaštenim osobama. Korisniku se preporučuje postavljanje jake *BIOS* zaporke. Detaljne preporuke oko izbora jake zaporke mogu se pročitati na web adresi http://www.cert.hr/filehandler.php?did=109.

5. Zaključak

Sigurnost stolnih i prijenosnih računala s Windows operacijskim sustavom podići će se na višu razinu pomoću preporuka koje su dane u dokumentu. Slijedom navedenih koraka korisnik će podesiti različite postavke kojima će utjecati na sigurnost računala i informacija, a funkcionalnost operacijskog sustava

neće biti ugrožena. Bitno je napomenuti da se početnicima ipak ne savjetuje samostalno podešavanje onih postavki s kojima nisu upoznati kako ne bi došlo do narušavanja funkcionalnosti sustava.

6. Reference

[1] Mandal, Arindam: Securing your Windows laptop
http://www.infosecwriters.com/text_resources/pdf/securing_your_laptop.pdf

[2] Microsoft Corporation: Step-by-Step Guide to Securing Windows XP Professional with Service Pack 2 in Small and Medium Businesses
http://download.microsoft.com/download/9/4/d/94dd17e2-1a63-4094-a560-e15bff312dfc/XPSP2SMB.pdf