CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Uklanjanje suvišnih mrežnih servisa na Windows sustavima

CCERT-PUBDOC-2002-11-06

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

Windows operacijski sustavi dolaze sa raznim mrežnim servisima koji se pokreću prilikom instalacije. U normalnim okolnostima, ukoliko sustav ne pruža mrežne usluge drugim računalima, iz sigurnosnog aspekta preporuča se onemogućavanje većine tih servisa.
Ovaj dokument opisuje neke servise koje je moguće ukloniti i načine na koje se to postiže. U dokumentu su opisani Windows 2000, odnosno XP sustavi, instalirani na uobičajeni način.

2. Identifikacija servisa

Najbrži način identifikacije mrežnih servisa je pregled popisa otvorenih TCP i UDP portova korištenjem `netstat` naredbe.
Sljedeći primjer prikazuje rezultat pokretanja `netstat` naredbe sa parametrima "`-an`" (prikaz svih spojeva i portova koji osluškuju, s prikazom adresa i portova u numeričkom obliku) na Windows 2000 sustavu:

```
C:\WINNT>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4983           0.0.0.0:0              LISTENING
  TCP    192.70.106.143:139     0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1028           *:*
  UDP    0.0.0.0:1029           *:*
  UDP    0.0.0.0:3456           *:*
  UDP    192.70.106.143:137     *:*
  UDP    192.70.106.143:138     *:*
  UDP    192.70.106.143:500     *:*
```

Na Windows XP sustavu korištenjem dodatnog parametra "`-o`" moguće je uz prikaz portova i adresa dobiti i popis odgovarajućih procesa koji koriste mrežne resurse:

```
C:\WINDOWS>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       884
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       976
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING       1160
  TCP    192.70.106.143:139     0.0.0.0:0              LISTENING       4
  UDP    0.0.0.0:135            *:*                                    884
  UDP    0.0.0.0:445            *:*                                    4
```

```
  UDP    0.0.0.0:500            *:*                                    704
  UDP    0.0.0.0:1026           *:*                                    1112
  UDP    0.0.0.0:1027           *:*                                    976
  UDP    127.0.0.1:123          *:*                                    976
  UDP    127.0.0.1:1900         *:*                                    1160
  UDP    192.70.106.143:123     *:*                                    976
  UDP    192.70.106.143:137     *:*                                    4
  UDP    192.70.106.143:138     *:*                                    4
  UDP    192.70.106.143:1900    *:*                                    1160
```

Ovdje valja spomenuti da `netstat` naredba ustvari ne prikazuje stvarno stanje TCP i UDP portova, već ustvari stanje TDI (*engl. Transport Driver Interface*) krajnjih točaka, što ne mora biti ekvivalentno pravom stanju TCP i UDP portova.
Npr., kada Windows sustav stvara odlazni TCP spoj, lokalni port koji se koristi biti će korištenjem `netstat` naredbe prijavljen kao "LISTENING".
Sljedeći primjer prikazuje uspostavu TCP spoja sa lokalnog (ishodišnog) porta 1367 na odredišni port 22 udaljenog sustava. Naredba `netstat` vraća sljedeći rezultat:

```
C:\WINDOWS>netstat -anp tcp | find ":1367"
  TCP    0.0.0.0:1367           0.0.0.0:0              LISTENING
  TCP    192.70.106.142:1367    192.70.106.76:22       ESTABLISHED
```

Drugi redak prikazuje uspostavljeni spoj od lokalnog porta 1367 prema udaljenom portu 22. No isto tako može se uočiti da prvi redak ispisa neispravno prikazuje stanje lokalnog porta 1367 ("LISTENING"), pošto na tom portu ne postoji nikakav TCP poslužiteljski servis.
Za svaki odlazni TCP spoj u ispisu `netstat` naredbe uvijek će se pojavljivati dodatni redak koji je odgovarajući TCP port prijavljivati u "LISTENING" stanju. Vrlo je važno uočiti razliku između otvorenog TCP porta i porta kojeg `netstat` nepravilno prijavljuje u "LISTENING" stanju. Ova pogreška postoji u svim implementacijama `netstat` naredbe osim unutar Windows .NET Server build 3606 i novijim.

3. Onemogućavanje servisa koji se ne koriste

Prvi korak u cilju minimiziranja broja otvorenih portova jest onemogućavanje servisa koji se ne koriste. Servisi se mogu zaustaviti korištenjem `net stop` naredbe, no prilikom restarta sustava servisi zaustavljeni na taj način biti će ponovno pokrenuti. Ukoliko se želi postići trajno zaustavljanje odgovarajućeg servisa potrebno je promijeniti način pokretanja u "*manual*" (ručno pokretanje) ili "*disabled*" (onemogućeno pokretanje servisa). Neke servise potrebno je eksplicitno onemogućiti jer ih u protivnom sustav sam pokreće korištenjem ručnog pokretanja.
Unutar Windows 2000 okruženja Service Manager omogućava podešavanje načina pokretanja servisa, dok u se Windows XP okruženju naredba za onemogućavanje servisa može koristiti naredba `sc` (također postoji u Windows 2000 Resource Kit paketu). Način korištenja naredbe je sljedeći (razmak poslije "start=" je obavezan):

```
C:\WINDOWS> sc config service_name start= disabled
C:\WINDOWS> sc config service_name start= manual
```

3.1. Windows 2000

3.1.1. IIS 5

Prilikom instalacije Windows 2000 operacijskog sustava automatski se pokreće i IIS 5 koji se sastoji od SMTP, HTTP i IIS administrativnih servisa. Da bi se zatvorili TCP portovi 25, 80 i 443, UDP port 3456, port namijenjen IIS administrativnom web poslužitelju (u ovom primjer 4983), te još dva dodatna visoka porta namijenjena RPC servisima potrebno je zaustaviti spomenute servise.

Najbrži način zaustavljanja tih servisa je zaustavljanje *IISadmin* servisa, pošto ostali spomenuti servisi direktno ovise o njemu.
Zaustavljanjem tog servisa trenutno će biti zaustavljeni sljedeći servisi:

- *World Wide Web Publishing Service*
- *Simple Mail Transfer Protocol (SMTP)*

Nakon zaustavljanja tih servisa rezultat pokretanja `netstat –an` naredbe prikazuje smanjeni broj otvorenih portova:

```
C:\WINNT>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    192.70.106.143:139     0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1029           *:*
  UDP    192.70.106.143:137     *:*
  UDP    192.70.106.143:138     *:*
  UDP    192.70.106.143:500     *:*
```

Naravno, najjednostavniji način onemogućavanja pokretanja IIS servisa jest uklanjanje IIS komponenti unutar *Add/Remove Programs* appleta u *Control Panel-u*.

3.1.2. IPSec

UDP port 500 koji koristi IKE (*engl. Internet Key Exchange*) protokol može biti zatvoren zaustavljanjem *IPsec Services* servisa:

```
C:\WINNT> net stop policyagent
The IPSEC Services service is stopping.
The IPSEC Services service was stopped successfully.
```

Nakon toga u prikazu otvorenih portova nestaje i port UDP 500:

```
C:\WINNT>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    192.70.106.143:139     0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1029           *:*
  UDP    192.70.106.143:137     *:*
  UDP    192.70.106.143:138     *:*
```

3.1.3. Distribution Transaction Coordinator

Distribution Transaction Coordinator je servis zadužen za povezivanje transakcija i transakcijskih komponenti sa različitih poslužitelja DTC poslužitelja. Servis se na Windows 2000 Server operacijskom sustavu automatski pokreće te otvara TCP port 3372 i još jedan visoki TCP port.
Servis je moguće zaustaviti na sljedeći način i tako zatvoriti još dva dodatna TCP porta:

```
C:\WINNT> net stop msdtc
The Distributed Transaction Coordinator service is stopping.
The Distributed Transaction Coordinator service was stopped successfully.
```

Popis otvorenih portova sad izgleda ovako:

```
C:\WINNT>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    192.70.106.143:139     0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1029           *:*
  UDP    192.70.106.143:137     *:*
  UDP    192.70.106.143:138     *:*
```

3.2. Windows XP

Na Windows XP postoji nekoliko servisa koje je moguće jednostavno onemogućiti:

- *IPSec Services* (PolicyAgent) koji služi za dohvaćanje informacija o IPSec politici te prosljeđivanje mehanizmima koji ih koriste,
- *SSDP Discovery Service* (SSDPSRV) koji služi da pronalaženje UPnP (*engl. Universal Plug and Play*) uređaja na mreži,
- *Windows Time* (W32Time) koji služi za vremensku sinkronizaciju zbog mogućih potreba *Kerberos* autentikacije.

Servise je moguće onemogućiti na sljedeći način:

```
C:\WINDOWS> net stop policyagent
The IPSEC Services service is stopping.
The IPSEC Services service was stopped successfully.


C:\>WINDOWS> net stop ssdpsrv
The SSDP Discovery Service service is stopping.
The SSDP Discovery Service service was stopped successfully.


C:\>WINDOWS> net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.
```

Nakon toga, naredba `netstat -ano` daje sljedeći rezultat:

```
C:\WINDOWS>netstat -ano

Active Connections
```

```
  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       884
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       976
  TCP    192.70.106.143:139     0.0.0.0:0              LISTENING       4
  UDP    0.0.0.0:135            *:*                                    884
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:1026           *:*                                    1112
  UDP    0.0.0.0:1027           *:*                                    976
  UDP    192.70.106.143:137     *:*                                    4
  UDP    192.70.106.143:138     *:*                                    4
```

4. NetBIOS over TCP/IP (NetBT)

NetBIOS over TCP/IP na Windows sustavima obično se koristi za prijenos CIFS (*engl. Common Internet File Services*) protokola, poznatog i pod imenom SMB (*engl. Server Message Block*). CIFS je protokol koji je zadužen za dijeljenje resursa (obično dijeljenje datoteka i pisača).
NetBIOS over TCP/IP koristi UDP portove 137 i 138, te TCP port 139. Da bi se ti portovi zatvorili *NetBIOS over TCP/IP* mora biti onemogućen na svakom mrežnom sučelju.
Onemogućavanje *NetBIOS over TCP/IP* moguće je kroz *Advanced TCP/IP Settings*, *WINS* kartica, *Disable NetBIOS over TCP/IP*. Na ovaj način zatvaraju se navedeni UDP i TCP portovi.
Lmhosts servis koji služi za pretvaranje NetBIOS imena također je moguće zaustaviti i onemogućiti:

```
C:\WINDOWS>net stop lmhosts

The TCP/IP NetBIOS Helper service was stopped successfully.
```

Nakon toga na Windows 2000 popis otvorenih portova izgleda ovako:

```
C:\WINNT>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1029           *:*
```

Na Windows XP popis je sljedeći:

```
C:\WINDOWS>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       884
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       976
  UDP    0.0.0.0:135            *:*                                    884
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:1026           *:*                                    1112
  UDP    0.0.0.0:1027           *:*                                    976
```

5. CIFS over TCP/IP

Prije pojave Windows 2000 operativnih sustava za prijenos CIFS protokola je bio zadužen *NetBIOS over TCP/IP* preko porta 139. U Windows 2000 CIFS se može prenositi direktno preko TCP/IP na portu 445, bez potrebe za dodatnim NetBT slojem.
Osluškivanje na TCP portu 445 može se onemogućiti na dva načina:

- onemogućavanjem NetBT *drivera*,
- dodavanjem vrijednosti u *registry* datoteku koja onemogućava prijenos CIFS preko TCP/IP.

U oba slučaja potreban je *restart* sustava, pošto NetBT *driver* otvara port 445 prilikom podizanja sustava. Preporuča se korištenje druge opcije, odnosno postavljanje sljedeće vrijednosti u *registry* datoteci:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters
Value: SmbDeviceEnabled
Type: DWORD value (REG_DWORD)
Content: 0 (to disable)
```

Nakon restarta TCP port 445 neće više biti otvoren.
Na Windows 2000 ostaju otvoreni sljedeći portovi:

```
C:\WINNT>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:1029           *:*
```

Na Windows XP preostali su sljedeći portovi:

```
C:\WINDOWS>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       884
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       976
  UDP    0.0.0.0:135            *:*                                    884
  UDP    0.0.0.0:1026           *:*                                    1112
  UDP    0.0.0.0:1027           *:*                                    976
```

6. RPC servisi

Preostale portove koriste RPC (*engl. Remote Procedure Call*) servisi. RPC *portmapper* i *COM Service Control Manager* (COM SCM) koriste port 135. Portove odmah iznad porta 1023 također koriste RPC servisi, i oba su dostupna preko RPC ili DCOM (ORPC). Ovi portovi alociraju se dinamički, te zahtijevaju postojanje *portmapper* servisa koji određuje na kojem portu se nalazi odgovarajući RPC servis. Popis registriranih RPC servisa u *portmapper* bazi može se pregledati korištenjem `rpcdump` alata (ne spada u standardne Windows alate).

6.1. Windows 2000

Korištenjem `rpcdump` alata može se vidjeti da RPC servisi koriste UDP port 1029 koji je pokrenut od strane *Messenger* servisa. Onemogućavanjem tog servisa i *restartom* računala zatvara se i taj port.

Također, UDP port 135 isto neće biti otvoren zato jer je i posljednji RPC servis dostupan preko UDP-a onemogućen, a isto tako DCOM nije dostupan preko UDP, tako da COM SCM ne osluškuje na UDP portu 135.
TCP port 1026 koriste RPC servisi koje pokreće *Task Scheduler* servis (*Schedule*). Onemogućavanjem tog servisa moguće je zatvoriti i taj port.
Remote Access Connection Manager (*RasMan*) također treba onemogućiti.

6.2. Windows XP

Na Windows XP sustavima UDP port 1027 koriste RPC servisi koje pokreće *Mesenger* servis. Kao i unutar Windows 2000, ovaj port isto kao i UDP port 135 biti će zatvoreni nakon onemogućavanja tog servisa i *restarta* računala.
TCP port 1025 koriste RPC servisi *Task Scheduler* servisa, ta kao i na Windows 2000, taj servis treba se onemogućiti.

7. Ograničavanje na sučeljima

U prethodnom poglavlju za zatvaranje dinamički alociranih portova onemogućavani su procesi koji pokreću RPC servise. Naravno, u nekim slučajevima pojedini servisi poput *Task Scheduler-a* su potrebni za normalno funkcioniranje sustava.
Jedno rješenje jest stvaranje dva dodatna ključa i jedne vrijednosti u *registry* datoteci. Na taj način RPC servise moguće je ograničiti da osluškuju samo ograničeni popis sučelja. Npr., moguće je ograničiti osluškivanje samo na *loopback* adresu `127.0.0.1` koje je dostupna jedino lokalno.
Sljedeći parametar određuje mrežna sučelja na kojima će RPC servisi biti dostupni. Mrežna sučelja identificiraju se brojevima počevši od broja 1. Vrijednost "0" predstavlja IP adresu `127.0.0.1`.
Dva ključa `Rpc\Linkage\` moraju biti napravljeni unutar `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`.
Vrijednost koju treba dodati jest:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rpc\Linkage
Value: Bind
Type: REG_MULTISZ
Content: "0"
```

Na sustavima starijim od Windows XP stvaranje vrijednosti tipa `REG_MULTISZ` moguće je samo korištenjem `regedt32` aplikacije. Nakon *restarta* računala TCP portovi koji osluškuju neposredno iznad porta 1023 biti će ograničeni na IP adresu `127.0.0.1`.

8. DCOM

Jedini preostali otvoreni port je TCP port 135. Taj port otvara *Remote Procedure Call* (*RpcSS*) servis koji se ne može onemogućiti pošto taj servis sadrži *COM Service Control Manager* koji koriste lokalni procesi.
TCP port 135 ostaje otvoren pošto se koristi za udaljene zahtjeve za aktivacijom COM objekata. Korištenjem `dcomcnfg` alata moguće je onemogućiti DCOM (*Enable Distributed COM on this computer* opcija), ali postavljanje te vrijednosti ne zatvara port 135.
Jedno rješenje je uklanjanje nizova RPC protokola koji se mogu koristiti unutar DCOM. U opisanom slučaju moguće je ukloniti `ncacn_ip_tcp` (prijenos korištenjem TCP/IP).
Najjednostavniji način da bi se to učinilo je pokretanje `dcomcfg` alata i uklanjanje *Connection-oriented TCP/IP* opcije unutar *Default Protocols* kartice. Pod Windows XP, `dcomcfg` pokreće MMC konzolu koja sadrži *Component Services* komponentu. Kartica Default Protocols može se pronaći unutar *Local System* svojstava.
Nakon *restarta* računala na Windows 2000 svi portovi trebali bi biti zatvoreni, dok kod Windows XP preostaje otvoren još jedan UDP port.

9. Caching DNS servis

Windows 2000 i noviji Windows sustavi u sebi uključuju *caching* DNS servis (*dnscache*) koji u memoriji čuva rezultate DNS upita.
Unutar Windows 2000 ovaj servis DNS zahtjeve šalje korištenjem UDP-a, tako da za svaki DNS zahtjev koristi drugi UDP port. Unutar Windows XP uvijek se koristi isti UDP port koji se alocira prilikom prvog DNS zahtijeva i koristi se sve dok je *dnscache* servis pokrenut. U primjeru port koji koristi *dnscache* je UDP port 1026. Zbog toga će jedan UDP port uvijek biti otvoren, dok god je *dnscache* servis pokrenut na računalu.

10. Zaključak

Minimiziranje mrežnih servisa moguće je postići kroz tri koraka:
- onemogućavanjem servisa koji se ne koriste,
- onemogućavanjem NetBIOS over TCP/IP, te CIFS over TCP/IP,
- minimiziranjem RPC servisa.

Servisi koje je općenito moguće onemogućiti su sljedeći na Windows 2000 su sljedeći:
- IIS 5 : iisadmin, w3svc, smtpsvc,
- ostali : *messenger*, *msdtc*, *policyagent*, *schedule*.

Na Windows XP moguće je onemogućiti sljedeće servise:
- *messenger*, *policyagent*, *schedule*, *ssdpsrv*, *w32time*.

Onemogućavanje *NetBIOS over TCP/IP* potrebno je podesiti za svako pojedino mrežno sučelje. Za općenito onemogućavanje *CIFS over TCP/IP* (port 445) potrebno je u *registry* datoteku dodati varijablu `SmbDeviceEnabled` i postaviti je na vrijednost "0".
Minimiziranje RPC servisa počinje onemogućavanjem servisa koji registriraju RPC servise. Nakon toga dvije postavke mogu dodatno ograničiti broj RPC servisa koji osluškuju na otvorenim portovima:
- postavljanjem varijable `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rpc\Linkage\Bind`, tipa `REG_MULTI_SZ`, na vrijednost "0",
- uklanjanjem *Connection-oriented TCP/IP* protokola korištenjem `dcomcfg` alata.

Neki RPC servisi mogu biti pokrenuti prilikom pokretanja pojedinih programa. Npr. *Component Services* komponenta unutar Windows XP otvara dva TCP porta koji koriste RPC servisi.
Zbog toga je osim tehnika minimiziranja opisanih u ovom dokumentu uvijek korisno korištenje IP filtriranja.
Standardno instalirani Windows sustavi pokreću mnoge mrežne servise koji se vrlo često ne koriste. Moguće je i poželjno u okruženjima koja zahtijevaju veću razinu sigurnosti minimizirati njihov broj, te ostaviti samo one servise koji su nužni.