Deaktivering af tjenester i Windows XP (første udgave og SP1)

E n standardinstallation af WinXP (Home og Pro) har flere netværkstjenester kørende, som desværre kan udnyttes af computerorme og andet snavs, som kan gøre livet surt for brugeren. Denne artikel er en kort gennemgang af de tjenester, man med fordel kan slå fra, for at sikre sin computer lidt bedre, inden den slippes løs på internettet ∞

Hvilke tjenester man har behov for afhænger af, hvad computerens rolle er, men i mit tilfælde drejer det sig om en enkeltstående computer, som ikke skal yde netværkstjenester til andre computere. Computeren skal bare have adgang til internettet via en ADSL-bredbåndsforbindelse (DHCP uden router og med dynamisk IP-adresse). Dog vil denne vejledning også beskrive, hvad der skal køre for at få et LAN til at fungere.

WinXP er nyinstalleret og netstikket er rykket ud af netkortet. Først når diverse netværkstjenester er lukket ned, bliver netstikket sat i. Erfaringen har vist mig, at man slipper for en del efterfølgende oprydningsarbejde, hvis man får lukket af for unødvendige tjenester, inden computeren får lov at komme på nettet.

Det første jeg plejer at gøre, på en frisk installeret WinXP, er at slukke for Systemgendannelse, Automatiske opdateringer(*), Fjernforbindelse og Fejlrapportering. Systemgendannelse er dog en god ting, da man har mulighed for at gå tilbage til et tidligere gemt gendannelsespunkt, hvis et eller andet går galt, men da jeg har valgt at investere i Drive Image fra Symantec, har jeg allerede lavet et image af installationen med Drive Image og har derfor ikke noget at bruge Systemgendannelse til. Om du vælger at slå funktionen fra eller ej er op til dig selv.

Systemgendannelse, Automatiske opdateringer og Fjernforbindelse findes inde i Kontrolpanel > System, som vist herude til højre. Under fanebladet Systemgendannelse er der sat et flueben i feltet "Deaktiver Systemgendannelse på alle drev". Under fanebladet Automatisk opdateringer er fluebenet "Hold computeren opdateret…" fjernet og under fanebladet Fjernforbindelse er fluebenet i "Tillad, at invitationer til fjernsupport sendes fra denne computer" også fjernet. Når det er gjort, går jeg i gang med at slukke for diverse netværkstjenester.

^(*) Dermed ikke sagt, at Automatiske opdateringer altid bør kobles fra. Jeg foretrækker blot at opdatere manuelt ved at besøge Windows Update-siden engang imellem.



Ved at starte en kommandoprompt og starte: netstat -an, kan man hurtigt få et overblik over, hvilke porte WinXP har åbnet op for ∞

c:\>netstat -an

Aktive forbindelser

Proto	Lokal adresse	Fjernadresse	Status
ТСР	0.0.0.0:135	0.0.0.0:0	LISTENING
ТСР	0.0.0.0:445	0.0.0.0:0	LISTENING
ТСР	0.0.0.0:1025	0.0.0.0:0	LISTENING
ТСР	0.0.0.0:5000	0.0.0.0:0	LISTENING
UDP	0.0.0.0:135	*:*	
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1026	*:*	
UDP	127.0.0.1:123	*:*	
UDP	127.0.0.1:1900	* *	

Start > Kør: services.msc starter Tjenester, som vist herude til højre. Find tjenesten IPSEC Policy Agent på listen, højreklik på den og vælg Egenskaber. Klik derefter på Stopknappen og stil den til Deaktiveret i feltet Starttype. Klik på OK for at lukke vinduet. Den ændring lukker for UDP:500.

Find SSDP-genkendelsestjenesten og gør det samme ved den (Stop, Deaktiver og OK). Det lukker for TCP:5000 og UDP:1900. En efterfølgende netstat -an i kommandoprompten, vil derfor resultere i følgende:

c:\>netstat -an

Aktive forbindelser

Proto	Lokal adresse	Fjernadresse	Status
ТСР	0.0.0.0:135	0.0.0.0:0	LISTENING
ТСР	0.0.0.0:445	0.0.0.0:0	LISTENING
ТСР	0.0.0.0:1025	0.0.0.0:0	LISTENING
UDP	0.0.0.0:135	* *	
UDP	0.0.0.0:445	* *	
UDP	0.0.0.0:1026	* *	
UDP	127.0.0.1:123	*:*	

Tjenesten Windows Time (UDP:123), sørger for at holde uret opdateret ved jævnligt at kontakte en tidsserver på internettet. Den funktion har jeg ikke brug for, så den deaktiveres ved først at dobbeltklikke på uret i proceslinjen og under fanebladet Internettid, fjernes fluebenet i "Synkroniser automatisk med en tidsserver på internettet". Derefter stoppes og deaktiveres tjenesten Windows Time inde i Tjenester (Start > Kør: services.msc).

iler Handling Vis					
	Hjælp				
• → 💽 🗗 🤄) 🖫 😫 🕨 🗖	■			
Tjenester (lokalt)	Navn			Beskrivelse	Sta V
	Hjælp og support	HØJREK	LIK	Aktiverer H Indeholder	Startet Startet
	Hændelseslog			Aktiverer h	Startet
	IPSEC Policy Agen	t Start		Styrer IP-si	Startet
	Logical Disk Manaç	ger Stop	and an	Registrerer	Startet
	Messenger	Fortsæt	rcialge	Overfører	Startet
	NLA (Network Loc	ation /Genstart		Indsamler o	Startet
	Opgavestyring	Alle opgav	er ▶	Gør det mul	Startet
	Plug and Play	Opdater		Aktiverer e Indlæser fil	Startet Startet
	Remote Procedure	e Call (<mark>Egenska</mark>	ber	Slutpunktsa	Startet
	Udvidet A Standar	d / Hjælp			
and the second					_
genskaber (Lo	kal compute	r) for IPSEC	Policy /	lgent	?
Navn på tienes	te: PolicyAgent	e Anængigne			
Vist navn:	IPSEC Policy	Agent			
Beskrivelse:	Styrer IP-sikk ISAKMP/Oal	erhedspolitik og kley (IKE) og IP	g starter dr -sikkerhed	iverne for I.	~
0.01	0				
Still eksekver	Suctors 2014 -	0110			
ENWINDOWS	voystem32\lsass	.exe			
Starthune	Deskliverst				**
этактуре:					×
	hr	2			
		A CONTRACTOR	- 10 - 10		
genskaber (Lo	okal compute	r) for SSDP-	genkend	lelsestje.	- 2
Generelt Log p	å Genoprettels	e Afhængighe	d		
3 P		1			
Navn på tjenes	te: SSDPSRV				
Vietness	SSDP-genke	endelsestieneste	,		
visi havn:	- Set gonite				
Beskrivelse:	Gør det mulig	jt at finde UPn F ∞rket	-enheder	på	~
	Infernmenterve	ZIKOL			\sim
Sti til eksekverl	par fil:				
Sti til eksekverl E:\WINDOWS	oar fil: \System32\svch	ost.exe -k Loca	IService		
Sti til eksekverl E:\WINDOWS	oar fil: \System32\svch	ost.exe -k Loca	IService		
Sti til eksekveri E:\WINDOWS Starttype:	bar fil: \System32\svch Deaktiveret	ost.exe -k Loca	IService		~
Sti til eksekverl E:\WINDOWS Starttype:	bar fil: \System32\svch Deaktiveret	ost.exe -k Loca	IService		~
Sti til eksekverl E:\WINDOWS Starttype:	bar fil: \System32\svch Deaktiveret	ost.exe -k Loca	IService		~
Sti til eksekveri E:\WINDOWS Starttype: Tjenestestatus:	bar fil: \System32\svch Deaktiveret Stoppet	ost.exe -k Loca	IService		~
Sti til eksekveri E:\WINDOWS Starttype: 	Dar fil: \System32\svch Deaktiveret Stoppet Stoppet	ost.exe -k Loca	IService	e	× ?
Sti til eksekverl E:\WINDOWS Starttype: Tjenestestatus: genskaber (Lo Generelt Loa p	bar fil: \System32\svch Deaktiveret Stoppet Stoppet bkal compute å Genoprettels	ost.exe -k Loca	IService	e	× ?(
Sti til eksekveri E:\WINDOWS Starttype: Tjenestestatus: genskaber (Lo Generelt Log p	bar fil: \System32\svch Deaktiveret Stoppet Stoppet å Genoprettelse	ost.exe -k Loca 	IService wws Time	e	▼ ?(
Sti til eksekveri E:\WINDDWS Starttype: Tjenestestatus: genskaber (Logp Generelt Logp Navn på tjenes	bar fil: \System32\svch Deaktiveret Stoppet skal compute å Genoprettelse te: W32Time	ost.exe -k Loca 	IService wws Tim	e	▼
Sti til eksekveri E:\WINDDWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes	bar fil: \System32\svch Deaktiveret Stoppet Stoppet å Genoprettelse te: W32Time	ost.exe -k Loca	IService	e	
Sti til eksekveri E:\WINDDWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn:	bar fil: \System32\svch Deaktiveret Stoppet Stoppet å Genoprettelse te: W32Time Windows Tin	ost.exe -k Loca r) for Windo e) Afhængighe	IService	e	
Sti til eksekveri E:\WINDDWS Starttype: Tjenestestatus: genskaber (Log Generelt Log p Navn på tjenes Vist navn: Beskrivelse:	bar fil: \System32\svch Deaktiveret Stoppet \$ kal compute \$ Genoprettelse te: W32Time Windows Tim Vedligehous	ost.exe -k Loca	IService	e ng på alle	▼
Sti til eksekveri E:\WINDDWS Starttype: Tjenestestatus: genskaber (Logp Navn på tjenes Vist navn: Beskrivelse:	bar fil: \System32\svch Deaktiveret Stoppet bkal compute å Genoprettelse te: W32Time Windows Tin Vedligeholde klienter og se	ost.exe -k Loca r) for Windo e Afhængighe ne r dato- og tidss; arvere på netvæ	IService wws Time ad wnkroniseri erket. Hvis	e ng på alle : denne	▼
Sti til eksekveri E:\WINDOWS Starttype: Tjenestestatus: genskaber (Lo Generelt Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri	Dar fil: \System32\svch Deaktiveret Stoppet Stoppet Stoppet bkal compute å Genoprettelse te: W32Time Windows Tin Vedligeholde klienter og se par fil:	ost.exe -k Loca r) for Windo e Afhængighe ne r dato- og tidssj rivere på netvæ	IService wws Time ad whkroniseri erket. Hvis	e ng på alle : denne	 ▼ ?
Sti til eksekveri E:\WINDOWS Starttype: Tjenestestatus: genskaber (Lo Generelt Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri E:\WINDOWS	bar fil: \System32\svch Deaktiveret Stoppet Stoppet Stoppet bkal compute å Genoprettelse te: W32Time Windows Tin Vedligeholde klienter og se par fil: \System32\svch	ost.exe -k Loca r) for Windo e Afhængighe re r dato- og tidss; arvere på netvær ost.exe -k netss	IService wws Time ad whkroniseri erket. Hvis zcs	e ng på alle denne	 ▼ ?
Sti til eksekveri E:\WINDOWS Starttype: Tjenestestatus: genskaber (Lo Generelt Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri E:\WINDOWS	bar fil: \System32\svch Deaktiveret Stoppet bkal compute å Genoprettelse te: W32Time Windows Tin Vedligeholde klienter og se bar fil: \System32\svch	ost.exe -k Loca r) for Windo e Afhængighe ne r dato- og tidssy arvere på netvæ ost.exe -k netsy	IService wws Time ad whkroniseri erket. Hvis rcs	e ng på alle : denne	?
Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri E:\WINDOWS Starttype:	bar fil: \System32\svch Deaktiveret Stoppet	ost.exe -k Loca r) for Windo e Afhængighe re r dato- og tidssy arvere på netvæ ost.exe -k netsv	IService wws Time ad whkroniseri erket. Hvis rcs	e ng på alle : denne	?
Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri E:WINDOWS Starttype:	Dear fil: \System32\svch Deaktiveret Stoppet	ost.exe -k Loca r) for Windo e Afhængighe r dato- og tidssy srvere på netvæ ost.exe -k netsy	IService wws Time ad whkroniseri arket. Hvis zcs	e ng på alle denne	?
Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri E:WINDOWS Starttype:	Dear fil: \System32\svch Deaktiveret Stoppet	ost.exe -k Loca	IService wws Time ad whkroniseri erket. Hvis rcs	e ng på alle denne	
Sti til eksekveri E:\WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri E:\WINDOWS Starttype: Tjenestestatus:	bar fil: \System32\svch Deaktiveret Stoppet bkal compute å Genoprettelse te: W32Time Windows Tin Vedligeholde klienter og se bar fil: \System32\svch Deaktiveret Stoppet	ost.exe -k Loca	IService wws Time ad whkroniseri erket. Hvis rcs	e ng på alle denne	
Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus:	bar fil: \System32\svch Deaktiveret Stoppet stoppet ster W32Time Windows Tin Vedligeholde klienter og se Dar fil: \System32\svch Deaktiveret Stoppet	r) for Windo	IService wws Time ad whkroniseri erket. Hvis rcs	e ng på alle : denne	
Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: Start	bar fil: \System32\svch Deaktiveret Stoppet bkal compute å Genoprettelse de: W32Time Windows Tin Vedligeholde klienter og se bar fil: \System32\svch Deaktiveret Stoppet	ost.exe -k Loca	IService wws Time ad ankroniseri arket. Hvis zcs dlertidigt	e ing på alle : denne	et
Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: Start Du kan angive	bar fil: \System32\svch Deaktiveret Stoppet bkal compute å Genoprettelse de W32Time Windows Tin Vedligeholde klienter og se bar fil: \System32\svch Deaktiveret Stoppet Stoppet	ost.exe -k Loca r) for Windo Afhængighe ne r dato- og tidssy srvere på netvæ ost.exe -k netsv Stop mid netre der skal a	IService wws Time ad whkroniserie arket. Hvis rcs dlertidigt nvendes,	e ing på alle denne Fortsa når du statte	
Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Vist navn: Beskrivelse: Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: Start Du kan angive tjenesten herfra	bar fil: \System32\svch Deaktiveret Stoppet bkal compute å Genoprettelse de W32Time Windows Tin Vedligeholde klienter og se bar fil: \System32\svch Deaktiveret Stoppet Stoppet	ost.exe -k Loca	IService	e ing på alle : denne Fortsa når du statte	
Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Vist navn: Beskrivelse: Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: Starttype: Du kan angive tjenesten herfre Startparametre:	bar fil: \System32\svch Deaktiveret Stoppet Stoppet Stoppet di Genoprettelse di Genoprettelse di Genoprettelse vedligeholde klienter og se par fil: \System32\svch Deaktiveret Stoppet Stoppet	ost.exe -k Loca r) for Windo Afhængighe ne r dato- og tidssy srvere på netvæ ost.exe -k netsv Stop mid netre der skal a	IService	e ing på alle : denne Fortsa når du statte	
Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Vist navn: Beskrivelse: Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: Starttype: Tjenestestatus: Start Du kan angive tjenesten herfra Startparametre:	bar fil: \System32\svch Deaktiveret Stoppet stoppet ster W32Time Windows Tin Vedligeholde klienter og se Dar fil: \System32\svch Deaktiveret Stoppet Stoppet	ost.exe -k Loca r) for Windo e Afhængighe ne r dato- og tidssy srvere på netvæ ost.exe -k netsv stop mid netre der skal a	IService	e ing på alle : denne Fortsa når du starte	
Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: genskaber (Log p Navn på tjenes Vist navn: Beskrivelse: Sti til eksekveri E:WINDOWS Starttype: Tjenestestatus: Starttype: Tjenestestatus: Start Du kan angive tjenesten herfra Startparametre:	bar fil: \System32\svch Deaktiveret Stoppet stoppet ster W32Time Windows Tin Vedligeholde klienter og se Dar fil: \System32\svch Deaktiveret Stoppet Stoppet	ost.exe -k Loca r) for Windo Afhængighe ne r dato- og tidss; srvere på netvæ ost.exe -k netsv Stop mid netre der skal a	IService	e ing på alle : denne Fortsa når du starte	

På denne side er beskrevet, hvad der skal køre for at få et LAN op at køre. Altså, et lokalt netværk imellem to eller flere computere. Hvis du ikke har brug for det, kan du springe denne side over og fortsætte på side 4. ∞

Ønsker man et LAN, kræver det, at man lader nogle tjenester køre, som rummer en vis risiko. Hvis man imidlertid benytter en router med NAT (det har de fleste) og en firewall (det har mange), så kan man godt have disse tjenester åbne, men en computer sat op på den måde, bør ikke sluttes direkte til internettet. I så fald kan man risikere at dele sin harddisk og filer med hele verden.

Klientprogram til Microsoft-netværk og fil- og udskriftsdeling skal være aktiverede, hvilket de er som standard. Du finder indstillingerne ved at gå i Start > Kontrolpanel > Netværks- og Internetforbindelser > Netværksforbindelser (eller blot Start > Indstillinger > Netværksforbindelser, hvis du kører med den klassiske startmenu), hvor du højreklikker på netværksforbindelsen og vælger Egenskaber.



Under fanebladet Generelt, finder du indstillingerne.

🕹 Egenskaber for LAN-forbindelse 🛛 🛛 🔀
Generelt Godkendelse Avanceret
Opret forbindelse ved hjælp af:
Bealtek RTL8139 Family PCI Fast Ethernet NIC
Konfigurer
Denne forbindelse bruger følgende elementer:
 Klientprogram til Microsoft-netværk Gudskriftsdeling til Microsoft-netværk QoS-pakkeplanlægning Thternetprotokol (TCP/IP)
Installer Fjern Egenskaber
Beskrivelse Giver computeren adgang til ressourcer på et Microsoft-netværk.

Ved at markere protokollen Internetprotokol (TCP/IP) og vælge Egenskaber, kommer følgende skærmbillede:

Egenskaber for Internetprotokol	(TCP/IP) ? 🔀
Generelt Alternativ konfiguration	
Du kan få IP-indstillinger tildelt automat denne facilitet. Ellers skal du kontakte få de korrekte IP-indstillinger.	isk, hvis dit netværk understøtter din netværksadministrator for at
⊙ Hent automatisk en IP-adresse	
🔿 Brug følgende IP-adresse: 🛛 —	
IP-adresse:	
Undernetmaske:	
Standardgateway:	
 Hent automatisk en DNS-serverar 	dresse
O Brug følgende DNS-serveradresse	er:
Foretrukken DNS-server:	
Alternativ DNS-server:	
	Avanceret

Ved at klikke på Avanceret og derefter WINS-fanebladet, kommer man ind til følgende vindue, hvor NetBIOS skal være koblet til. Derudover skal tjenesten TCP/IP NetBIOS Helper også køre, hvilket den også gør som standard.

Avancerede TCP/IP-indstillinger
IP-indstillinger DNS WINS Indstillinger
WINS-adresser i anvendelsesrækkefølge:
t
3
Tilføj Rediger Fjern
Hvis LMHOSTS-opslag er aktiveret, gælder det for alle forbindelser, hvor TCP/IP er aktiveret.
Aktiver LMHOSTS-opslag Importer LMHOSTS
← NetBIOS-indstilling
 Standard: Brug NetBIOS-indstilling fra DHCP-serveren. Hvis der bruges en statisk IP-adresse, eller hvis DHCP-serveren ikke angiver NetBIOS-indstillingen, skal NetBIOS aktiveres over TCP/IP.
O Aktiver NetBIOS over TCP/IP
O Deaktiver NetBios over TCP/IP
OK Annuller

Vis du ikke har behov for et LAN, kan Klientprogram til Microsoft-netværk, Fil- og udskriftsdeling til Microsoft-netværk samt NetBIOS over TCP/IP kobles fra, for de er ikke nødvendige for at få en enkeltstående computer på internettet. Disse kobles fra inde i Start > Kontrolpanel > Netværks- og Internetforbindelser > Netværksforbindelser (eller blot Start > Indstillinger > Netværksforbindelser, hvis du kører med den klassiske startmenu). Højreklik på netværksforbindelsen og vælg Egenskaber.

Fluebenet i Klientprogram til Microsoft-netværk og Filog udskriftsdeling til Microsoft-netværk fjernes og QoSpakkeplanlægning afinstalleres evt. også, da de færreste har programmer installeret, som understøtter den funktion. Derefter markeres Internetprotokol (TCP/IP) og der klikkes på Egenskaber. Under fanebladet Generelt klikkes der på Avanceret og under fanebladet WINS fjernes fluebenet i "Aktiver LMHOSTS-opslag" og "Deaktiver NetBIOS over TCP/IP" kobles til.



🕹 Egenskaber for LAN-forbindelse 🛛 🛛	?×
Generelt Godkendelse Avanceret	3
Opret forbindelse ved hjælp af:	
👜 Realtek RTL8139 Family PCI Fast Ethernet NIC	
Kopfgure	51
Denne forbindelse bruger følgende elementer:	·
🗆 🔜 Klientprogram til Microsoft-netværk	
El- og udskriftsdeling til Microsoft-netværk	
Installer Fjern Egenskaber	
Beskrivelse TCP/IP (Transmission Control Protocol/Internet Protocol)	
Egenskaber for Internetprotokol (TCP/IP)	?×
Generelt Alternativ konfiguration	4
Du kan få IP-indstillinger tildelt automatisk, hvis dit netværk understøtte denne facilitet. Ellers skal du kontakte din netværksadministrator for at få de korrekte IP-indstillinger.	я
● Hent automatisk en IP-adresse	
O Brug følgende IP-adresse:	
Undernetmaske:	
 Hent automatisk en DNS-serveradresse 	
Brug følgende DNS-serveradresser:	
Alternativ DNS-server	
Avancerel	
OK An	
Avancerede TCP/IP-indstillinger	? <mark>×</mark>
IP-indstillinger DNS WINS Indstillinger	5
WINS-adresser i anvendelsesrækkefølge:	_
Tilføj Rediger Fjern	
Hvis LMHOSTS-opslag er aktiveret, gælder det for alle forbindelser, hv TCP/IP er aktiveret.	'or
Aktiver LMHOSTS-opslag	
Real IDS-indstilling	
 Standard: Brug NetBIOS-indstilling fra DHCP-serveren. Hvis der bruges er statisk IP-adresse, eller hvis DHCP-serveren ikke angiver NetBIOS-indstillingen, skal NetBIOS aktiveres over TCP/IP. 	n
O Aktiver NetBIOS over TCP/IP	
Deaktiver NetBios over TCP/IP	
OK An	nuller

💶 🗖 🔀

CP:445 holdes åben til SMB/CIFS-protokollen.

Man kan vælge helt at frakoble NetBIOS over TCP/IPdriveren (NetBT), men da tjenesten DHCP-klientprogram, som jeg har brug for, er afhængig af, at NetBT-driveren kører, vælger jeg i stedet at tilføje en værdi til registreringsdatabasen, som slår SMB-transporten over TCP:445 fra uden at frakoble NetBT-driveren. Dette gøres ved at gå ned i Start > Kør og starte: regedit.

Når man er inde i nøglen [HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\NetBT\Parameters], højreklikker man ovre i højre side og vælger punktet Ny > DWORD-værdi. Den nye værdi kaldes: SmbDeviceEnabled. Sørg for at værdien står til 0 og luk så regedit.

Messenger-tjenesten er afhængig af NetBIOS, så den virker ikke efter NetBIOS over TCP/IP er koblet fra, hvilket som regel er en fordel, da det er blevet ret populært at sende spam til Messenger-tjenesten. Selvom den ikke virker uden NetBIOS, holder den dog stadig nogle porte åben, så man kan med fordel deaktivere Messenger-tjenesten helt (med services.msc), så den ikke starter sammen med Windows.

Det samme er tilfældet med tjenesten Opgavestyring / Task Scheduler (TCP:1025 i dette eksempel). Den tjeneste har jeg valgt at deaktivere, da ingen af mine programmer bruger den. Hvis man oplever problemer ved at have den deaktiveret, kan man jo altid stille den til Automatisk igen. (Visse tredjepartsprogrammer, som f.eks. antivirusprogrammers automatiske opdateringsfunktion, kan være afhængig af, at Opgavestyring kører).

Når Messenger og Opgavestyring er deakiveret genstartes computeren og efter genstarten, vil netstat -an i en kommandoprompt vise dette:

c:\>netstat -an

Aktive forbindelser

Proto	Lokal adresse	Fjernadresse	Status
ТСР	0.0.0.0:135	0.0.0.0:0	LISTENING

Hvis du oplever, at der holdes en TCP-port mere åben udover TCP:135 (f.eks. TCP:1025), så kan det være tjenesten Remote Access Connection Manager. Hvis det er tilfældet, kan du deaktivere den tjeneste, men du skal være opmærksom på, at hvis du har netværksforbindelser oprettet, som forbinder via et analogt modem eller en ISDN-adapter, vil disse forbindelser forsvinde inde fra Netværksforbindelser (de forsvinder først efter en genstart af Windows). Hvis du har sådanne forbindelser oprettet, eller har planer om at oprette dem på et senere tidspunkt, vil det derfor være



Egenskaber (Loka	l computer) for Messenger	?×
Generelt Log på	Genoprettelse Afhængighed	
Navn på tjeneste:	Messenger	
Vist navn:	Messenger	-
Beskrivelse:	Dverfører net send- og meddelelser fra tjenesten Alerter mellem klienter og servere. Denne tjeneste er	~
Sti til eksekverbar E:\WINDOWS\Sy	fil: istem32\svchost.exe -k netsvcs	_
Starttype:	Deaktiveret	~
Egenskaber (Loka	al computer) for Opgavestyring	? 🛛
Generelt Log på	Genoprettelse Afhængighed	
Navn på tjeneste:	Schedule	
Vist navn:	Opgavestyring	-
Beskrivelse:	Gør det muligt for en bruger at konfigurere og planlægge automatiserede opgaver på denne	~
Sti til eksekverbar E:\WINDOWS\Sy	fil: Istem32\svchost.exe -k netsvcs	_
Starttype:	Deaktiveret	~
Tjenestestatus:	Stoppet	-
Start	Stop Stop midlertidigt Fortsæt	
Du kan angive, hv tjenesten herfra.	ilke startparametre der skal anvendes, når du starter	
Startparametre:		
	OK Annuller A	nvend

SIDE 5

klogest at lade den tjeneste køre, men da jeg kun har brug for en LAN-forbindelse, vælger jeg at deaktivere Remote Access Connection Manager, for en sådan netværksforbindelse forsvinder ikke ved at deaktivere den tjeneste.

TCP:135 holdes aktiv af RPC (Remote Procedure Call) og RPC kan ikke kobles fra på WinXP, da den er en slags moder over alle tjenester, hvilket vil sige, at alle kørende tjenester er afhængige af RPC. Desværre er det sikkerhedshuller i netop RPC, som mange af dagens computerorme forsøger at snige sig ind af (blaster-ormen f.eks.) Heldigvis er der mulighed for at konfigurere WinXP, så RPC får lov at køre, men uden at TCP:135 åbnes og det kan bla. gøres med værktøjet Komponenttjenester.

Start > Kør: dcomcnfg skulle gerne resultere i, at vinduet Komponenttjenester kommer frem på skærmen. I det vindue højreklikkes der på Denne computer under punktet Komponenttjenester > Computere og punktet Egenskaber vælges.

Under fanebladet Standardegenskaber fjernes fluebenet ud for "Aktiver DCOM på denne computer" og under fanebladet Standardprotokoller fjernes protokollen Forbindelsesorienteret TCP/IP.

Inden den sidste genstart, vælger jeg at deaktivere tjenester (med services.msc), som jeg med garanti ikke har behov for og det drejer sig om følgende tjenester i mit tilfælde:

Alerter DNS-klient (DTC) Distributed Transaction Coordinator Tjenesten TCP/IP NetBIOS Helper (hvis NetBIOS over TCP/IP ikke køres. Se evt. side 3 & 4). Remote Registry Serienummer for bærbart medie Automatiske opdateringer (fordi jeg foretrækker at opdatere via Windows Update, som skrevet nederst på side 1).

Efter en genstart, vil netstat -an i kommandoprompten vise dette:

c:\>netstat -an

Aktive forbindelser

Proto Lokal adresse

Fjernadresse Status

Du skal være opmærksom på, at RPC stadig kan finde på at åbne TCP:135. Det kan ske, hvis du f.eks. starter dcomcnfg. RPC vil i så fald blive ved med at holde TCP:135 åben indtil næste genstart.

🏷 Komponenttjenester 📃 🗖 🗙
🕼 Filer Handling Vis Vindue Hjælp
Rod for konsol Computere 1 objekt(er)
Enne computer Denne computer
Stop MS DTC
Opdater alle komponenter
Vis P
Egenskaber
Feenskaber for Danna computer
Standardprotokoller MSDTC COM-standardsikkerhed
Generelt Indstillinger Standardegenskaber
⊢ Aktiver DCOM på denne computer
The tiver COM Internet Services på denne computer
Standardegenskaber for DCDM
Bodkendelsesniveauet angiver sikkerheden nå pakkeniveau
Standardniveau for godkondalka
Standaluniveau iui yuukenueise.
Egenskaber for Denne computer
Generelt Indstillinger Standardegenskaber
Standardprotokoller MSDTC COM-standardsikkerhed
DCOM-protokoller
Forbindelsesorienteret TCP/IP
Forbindelsesorienteret SFX
Tilføj Fjern Flyt op Flyt nedad Egenskaber
Beskrivelse
Egenskaber for Denne computer
Generelt Indstillinger Standardegenskaber
Standardprotokoller MSDTC COM-standardsikkerhed
DCOM-protokoller
Forbindelsesorienteret SPX
1
Tilføj Fjern Flyt op Flyt nedad Egenskaber
Beskrivelse
Det sæt netværksprotokoller, som er tilgængeligt for DCOM på denne computer. Protokolrækkefølgen angiver protokollernes indhurdes
prioritet. Den øverste protokol har førsteprioritet og vil blive anvendt
1 <i>0</i> 131.

 $R^{\rm PC's}$ åbning af TCP:135 kan forhindres vha. en værdi i registreringsdatabasen, som tvinger den til ikke at lytte på internettet. Hvis du ønsker at tilføje den værdi, kan du gå ned i Start > Kør og starte regedit.

Find følgende nøgle: [HKEY_LOCAL_MACHINE\SOFT-WARE\Microsoft\Rpc]. Når du har fundet den, højreklikker du på Rpc og vælger Ny > Nøgle (se øveste screenshot herude til højre). Den nye nøgle kaldes for internet (bemærk forskellen på store og små bogstaver).

Når internet-nøglen er oprettet, sørger du for at den er valgt og klikker derefter ovre i højre side af vinduet, hvor du vælger Ny > Strengværdi. Den nye strengværdi kaldes for UseinternetPorts. Højreklik derefter på den nye strengværdi, vælg Rediger og skriv no i feltet Værdidata. Klik på OK og luk registreringseditoren.

Jeg har endnu ikke oplevet problemer ved at have UseinternetPorts stillet til no for RPC inde i registreringsdatabasen. Det eneste lille minus er, at logbogen (Start > Kør: eventvwr.msc) vil komme med en advarsel (hændelses-id: 4358) og en fejl (hændelses-id: 4156) under kategorien Program, hvis man starter et program eller en funktion, som normalt ville få RPC til at åbne TCP:135. Hvis du oplever problemer med den indstilling, kan du blot slette internet-nøglen inde i [HKEY_LOCAL_MACHINE\SOFT-WARE\Microsoft\Rpc] og genstarte. Så er du tilbage til standardindstillingen.

Netkablet kobles til netkortet og computeren kan nu få lov til at komme på nettet. Det første man bør gøre er at besøge Windows Update og hente diverse sikkerhedsopdateringer og fejlrettelser og dette kan nu gøres i fred og ro uden at blive inficeret med diverse blaster-varianter, spammet med Messenger-spam osv. Det er en god idé at besøge Windows Update-siden ofte, for der bliver jævnligt udsendt sikkerhedsopdateringer.

Til dem som ønsker at gøre WinXP endnu sikrere, kan følgende PDF anbefales (den er på engelsk): http://www.giac.org/practical/GSEC/Zach_Groves_GSEC.pdf På side 16 i ovenstående PDF er der omtalt to VBS-filer (Tcpip_sec.vbs og Winsock.vbs), som kan hjælpe med til at styrke TCP/IP og winsock. Hvad disse to filer ændrer i registreringsdatabasen er nævnt på side 16 i ovenstående PDF og i Microsofts "Treats and Countermeasures Guide: Security Settings in Windows Server 2003 and Windows XP". De to VBS-filer kan hentes på følgende adresse: http://home18.inet.tele.dk/madsen/winxp/tcpip_winsock.zip

Tak til brugerne af gruppen dk.edb.sikkerhed for hjælpen til indholdet af dette dokument.

