Deaktivering af tjenester i Windows XP SP2 (Home eller Pro)

Mange vil nok mene, at den nye firewall i SP2 er beskyttelse nok i sig selv, men der kører stadig netværkstjenester, som de færreste brugere har behov for og ved at deaktivere dem, kan det kun blive til en sikrere og ikke mindst hurtigere Windows

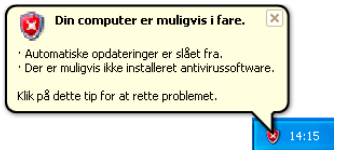
Hvilke tjenester man har behov for afhænger af, hvad computerens rolle er. I mit tilfælde drejer det sig om en enkeltstående computer, som ikke skal yde netværkstjenester til andre computere. Computeren skal bare have adgang til internettet via en ADSL-bredbåndsforbindelse (DHCP uden router og med dynamisk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

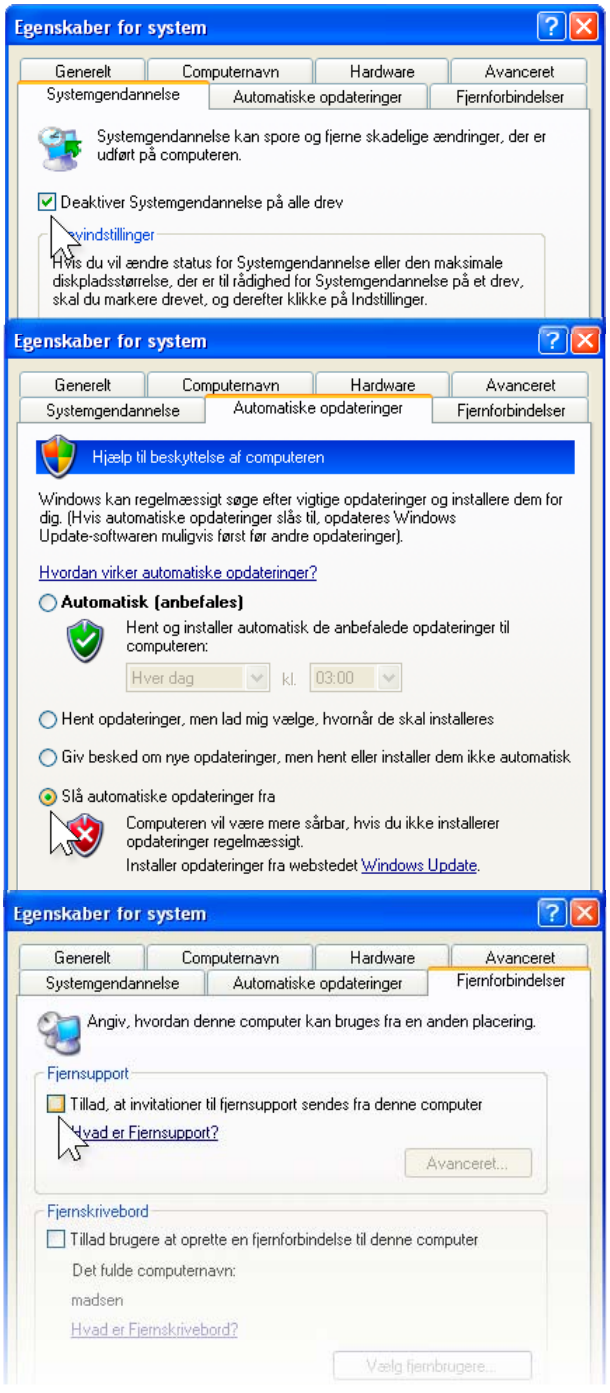
Det første jeg slukker for på en frisk installeret WinXP SP2 med netstikket rykket ud, da jeg helst vil undgå internetforbindelse indtil diverse netværkstjenester er deativeret, er Systemgendannelse, Automatiske opdateringer(*), Fjernforbindelse og Fejlrapportering. Med systemgendannelse har man mulighed 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 det program, 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 > Ydelse og vedligeholdelse > System (eller Kontrolpanel > System, hvis du bruger det klassiske kontrolpanel).

Under fanebladet Systemgendannelse er der sat et flueben i feltet „Deaktiver Systemgendannelse på alle drev". Under fanebladet Automatisk opdateringer er fluebenet sat i „Slå automatiske opdateringer fra"(*) og under fanebladet Fjernforbindelse er fluebenet i „Tillad, at invitationer til fjernsupport sendes fra denne computer" også fjernet.

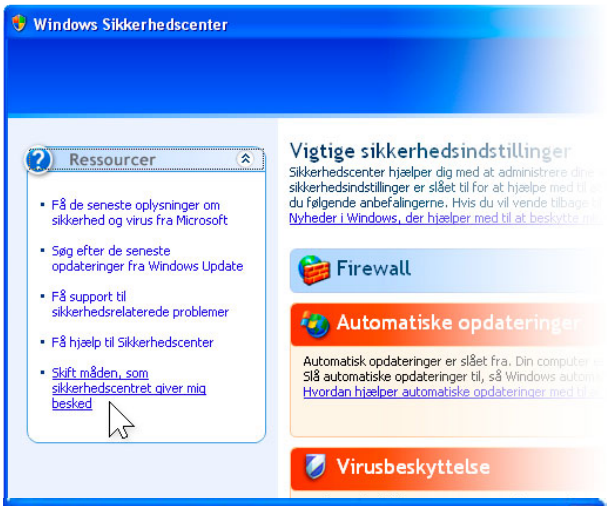
Når automatiske opdateringer kobles fra, vil det nye såkaldte sikkerhedscenter straks gøre opmærksom på det, ved at vise en gul advarselsboks i proceslinjen.





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

Advarslen fra sikkerhedscentret er i mine øjne irriterende at se på, så jeg vælger at klikke på det gule skilt, eller det røde ikon ved siden af uret, hvilket åbner sikkerhedscentret. Ovre i venstre side klikker jeg på punktet „Skift måden, som sikkerhedscentret giver mig besked" og fjerner fluebenet ved „Automatisk opdateringer" og „Virusbeskyttelse", da jeg heller ikke har noget antivirussoftware installeret på nuværende tidspunkt. Når der klikkes på OK, forsvinder den gule advarselsboks og det røde ikon fra sikkerhedscentret på proceslinjen. Derefter begynder jeg at deaktivere unødvendige netværkstjenester.



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

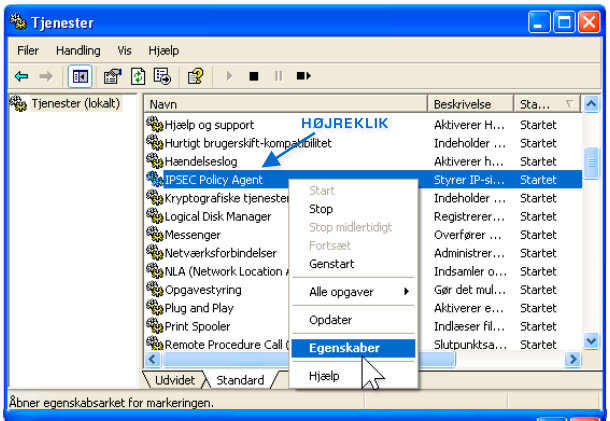
c:\>netstat -an

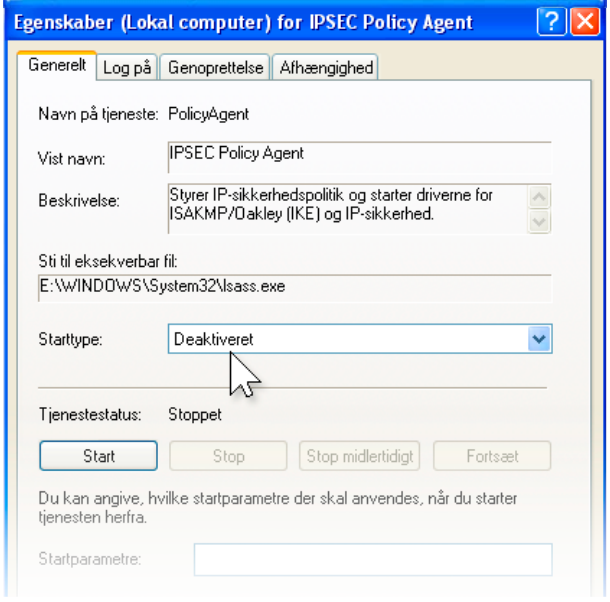
Aktive forbindelser

Proto	*Lokal adresse*	*Fjernadresse*	*Status*
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	*127.0.0.1:1028*	*0.0.0.0:0*	*LISTENING*
UDP	*0.0.0.0:445*	*:*	
UDP	*0.0.0.0:500*	*:*	
UDP	*0.0.0.0:4500*	*:*	
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 Stop-knappen og stil den til Deaktiveret i feltet Starttype.

Find SSDP-genkendelsestjenesten og gør det samme ved den. En efterfølgende netstat -an i kommandoprompten, vil nu vise følgende. UDP:500, UDP:4500 og UDP:1900 er forsvundet fra listen.



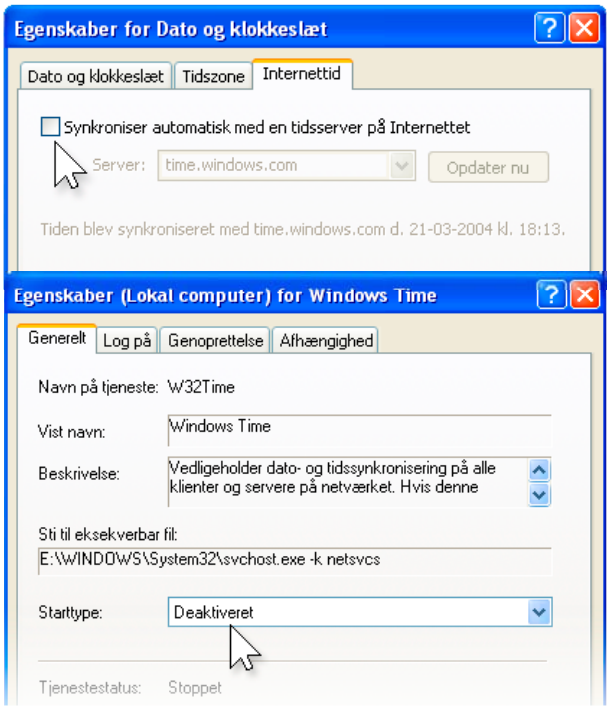


c:\>netstat -an

Proto	*Lokal adresse*	*Fjernadresse*	*Status*
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	*127.0.0.1:1028*	*0.0.0.0:0*	*LISTENING*
UDP	*0.0.0.0:445*	*:*	
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). Det får UDP:123 til at lukke.

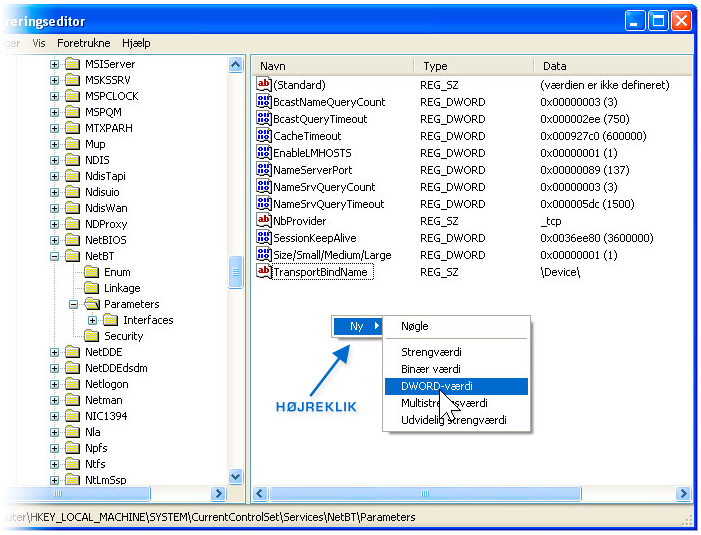


TCP:1028 i dette eksempel (portnummeret kan variere) er tjenesten Gatewaytjeneste til programlaget (Alg.exe) og vi kan se i netstat, at den kun tager imod lokale forbindelser (127.0.0.1 er vores egen computer), så den er knap så farlig.

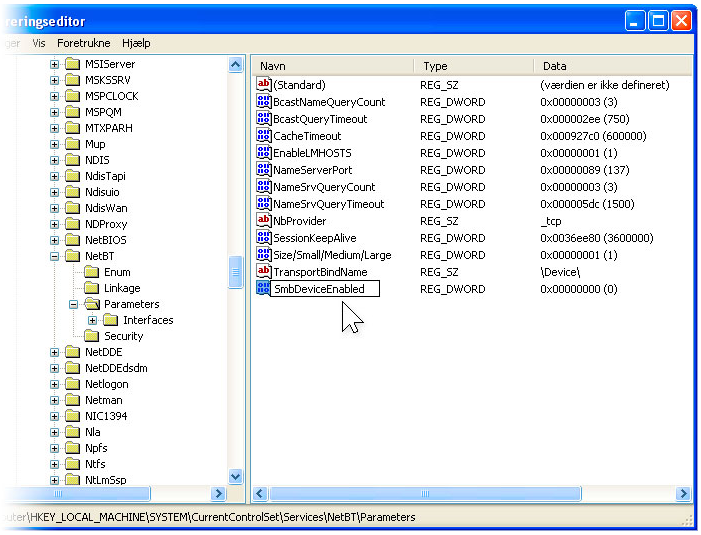
XP's firewall bruger tjenesten til installation af tredjeparts-plugins fra andre programmer på computeren, som skal kunne fungere sammen med firewallen på den ene eller den anden måde, så hvis du har planer om at bruge den indbyggede firewall, er det nok klogest at lade gatewaytjeneste til programlaget køre. Hvis du derimod hellere vil bruge en firewall fra en anden producent, eller måske slet ingen, kan du roligt deaktivere den tjeneste.

TCP:445 holdes åben til SMB/CIFS-protokollen.
Man kan vælge helt at frakoble NetBIOS over TCP/IP-driveren (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 og genstart computeren.



Efter en genstart, vil netstat -an vise dette:



c:\>netstat -an

Proto	*Lokal adresse*	*Fjernadresse*	*Status*
TCP	*0.0.0.0:135*	*0.0.0.0:0*	*LISTENING*
TCP	*127.0.0.1:1025*	**:**	

Gatewaytjeneste til programlaget har skiftet til TCP:1025 og TCP:135 holdes åben af RPC (Remote Procedure Call).

RPC-tjenesten 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 den. Desværre er det sikkerhedshuller i netop RPC, som mange af dagens computerorme forsøger at snige sig ind af.

Det skal dog siges, at Microsoft har forbedret sikkerheden i RPC i SP2. Efter sigende skulle det ikke længere være muligt for ondsindet kode at logge anonymt på RPC og firewallen skulle vel også gerne advare, hvis noget forsøger at forbinde til den, men alligevel foretrækker jeg nu at begrænse RPC's aktivitet så meget som muligt, da det i mit tilfælde ikke er nødvendigt, at den står og venter på forbindelsesforsøg udefra. Desuden er det jo ikke nemt at vide, hvad der sker den dag, hvor firewallen ikke længere beskytter RPC, fordi ondsindet kode har handlingslammet firewallen.

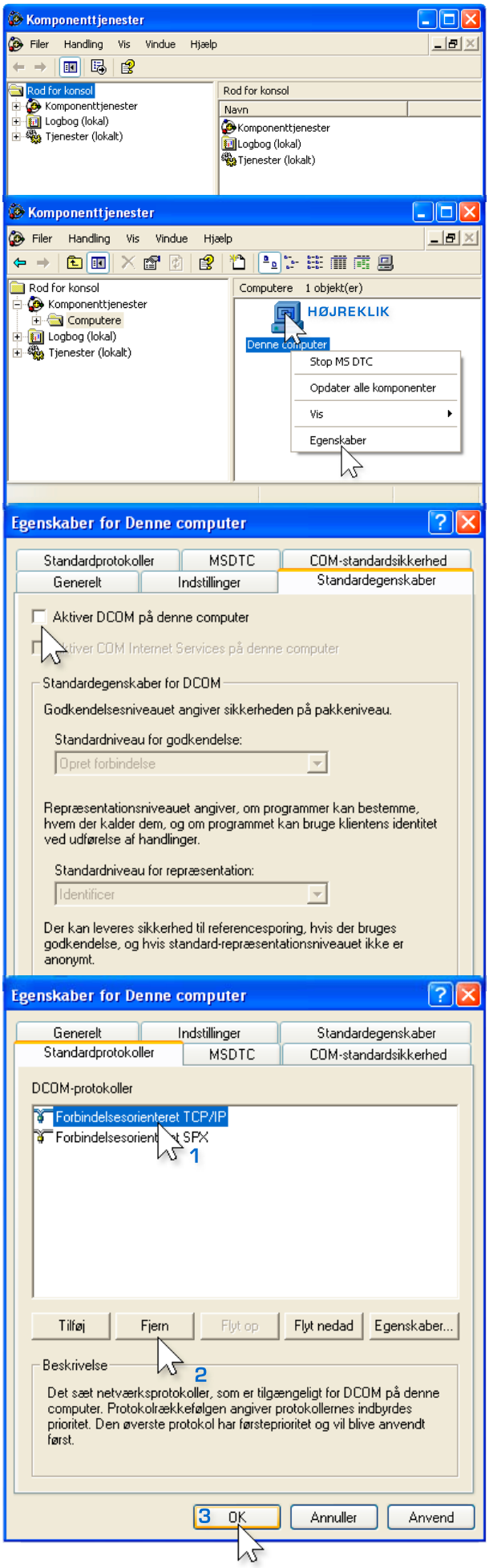
Man kan konfigurere WinXP, så RPC får lov at køre, men uden at TCP:135 åbnes, medmindre der er behov for det, og det kan bla. gøres med værktøjet Komponenttjenester, som kan startes via Start > Kør: dcomcnfg eller via Kontrolpanel > Ydelse og vedligeholdelse > Administration, hvor du i øvrigt også finder Tjenester (services.msc).

Når du starter Komponenttjenester første gang og klikker på plus-tegnet ud for Komponenttjenester under Rod for konsol, vil XP's firewall sikkert komme op med en advarsel om, at den har blokeret for nogle funktioner i Microsoft Mangement Console (MMC), som vist herunder. Jeg klikker på „Fortsæt blokering" og Komponenttjenester åbner.

Inde i vinduet Komponenttjenester 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", hvorefter der klikkes på OK for at lukke Komponenttjenester.

Hvis vi genstarter nu, vil TCP:135 være lukket efter genstarten, men RPC kan stadig finde på at åbne TCP:135. Det kan f.eks. ske, hvis du starter dcomcnfg igen på et senere tidspunkt. RPC vil i så fald blive ved med at holde TCP:135 åben indtil næste genstart. Det er derfor firewallen brokker sig, når du åbner dcomcnfg.



RPC's åbning af TCP:135 kan forhindres vha. en værdi i registreringsdatabasen, som tvinger den til ikke at lytte på Internettet, hvilket sjældent er nødvendigt. Hvis du ønsker at tilføje den værdi, kan du gå ned i Start > Kør og starte regedit.

Find følgende nøgle: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc]. Når du har fundet den, højreklikker du på Rpc og vælger Ny > Nøgle (se screenshottet øverst 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.

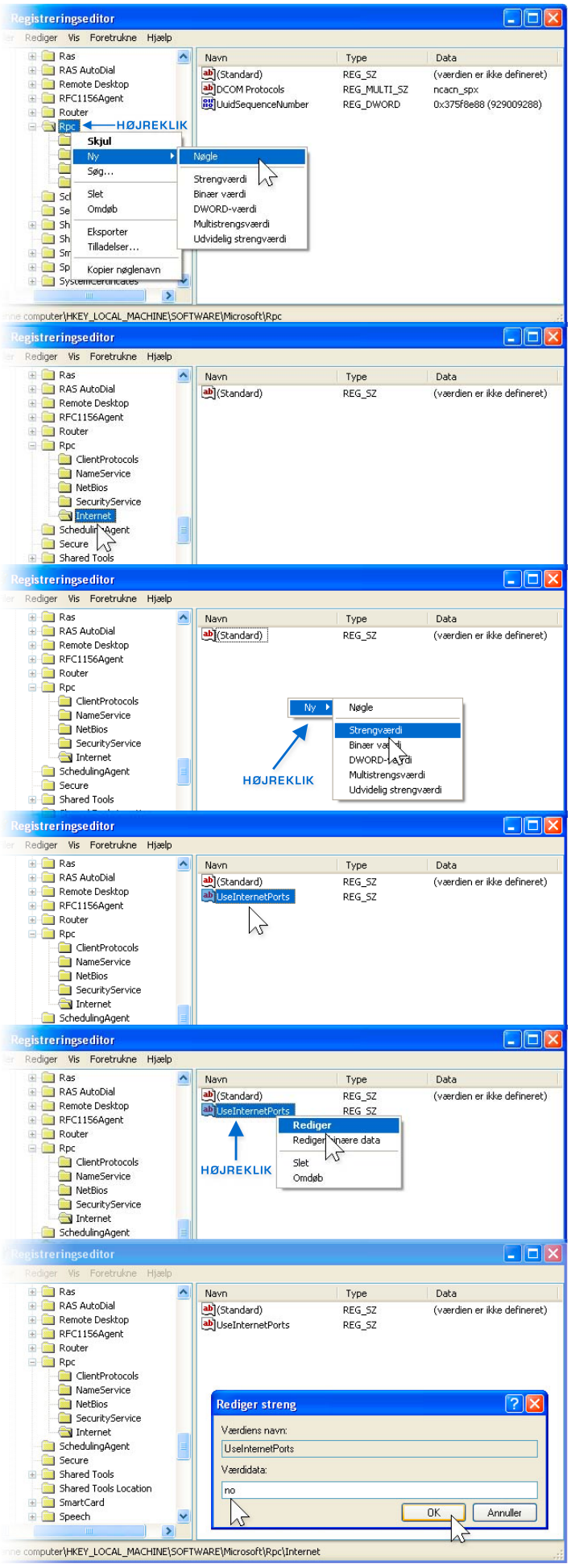
Jeg har endnu ikke oplevet problemer ved at have UseInternetPorts stillet til no for RPC inde i registreringsdatabasen. Det eneste lille minus er, at logbogen (Start > Kør: eventvwr.msc) vil komme med en advarsel (hændelses-id: 4358) og en fejl (hændelses-id: 4156) under kategorien Program, hvis man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

Efter endnu en genstart, viser netstat -an i kommandoprompten dette:

c:\>netstat -an

Proto	*Lokal adresse*	*Fjernadresse*	*Status*
TCP	*127.0.0.1:1025*	**:**	

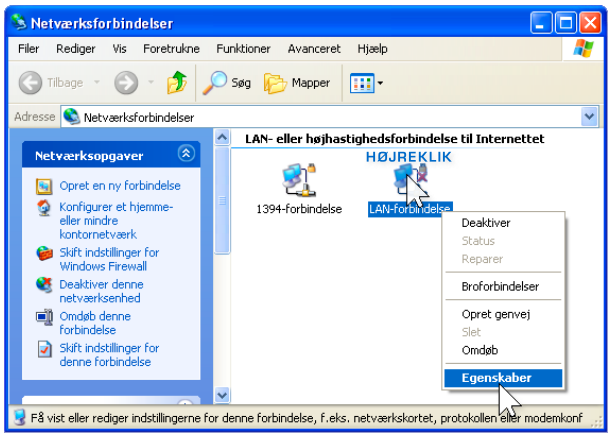
Det eneste vi har tilbage på listen er Gatewaytjeneste til programlaget. Den indbyggede firewall kan sagtens køre uden, men der kan opstå situationer, hvor firewallen ikke fungerer efter hensigten, hvis du deaktiverer den tjeneste. Det kommer an på, hvilke ekstra sikkerhedsprogrammer, du installerer, så det er svært at give nogle faste retningslinjer for, om du behøver tjenesten eller ej.



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 7.

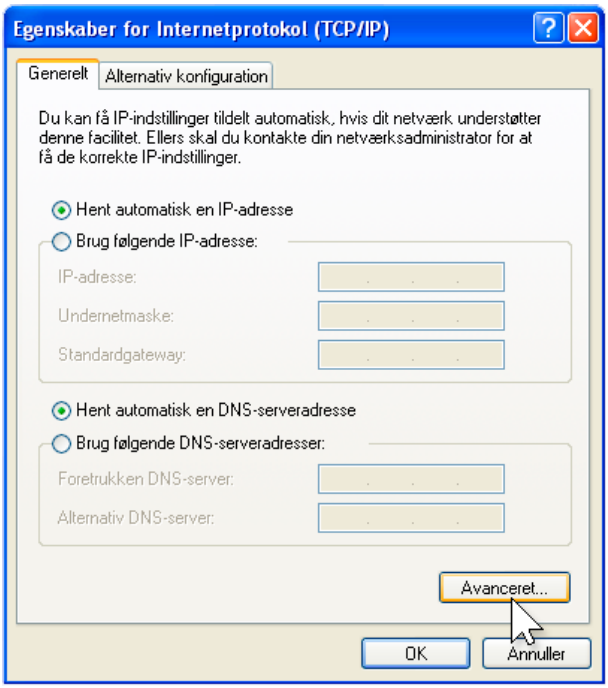
Ønsker man et LAN, kræver det, at man lader nogle tjenester køre, som rummer en vis risiko. Hvis man imidlertid benytter en router med NAT (det har de fleste) og en firewall (det har mange), så kan man godt have disse tjenester åbne, men en computer sat op på den måde, bør ikke sluttes direkte til internettet.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

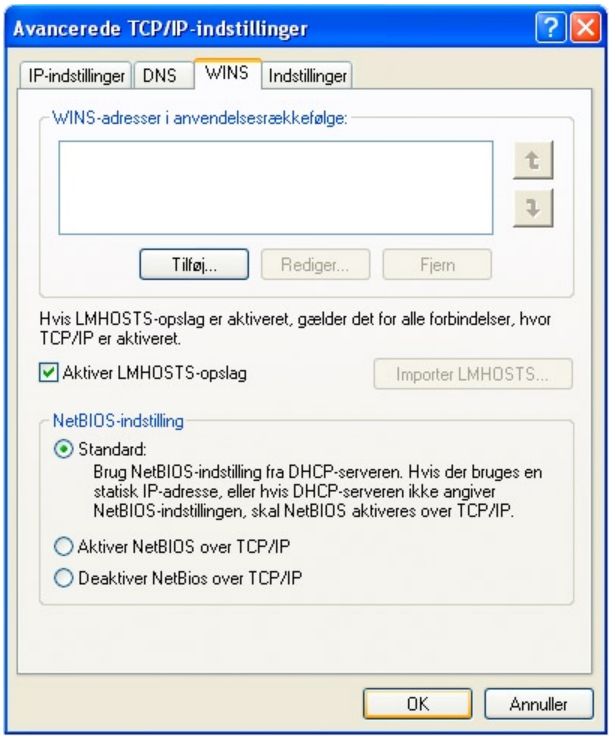


Under fanebladet Generelt, finder du indstillingerne.

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

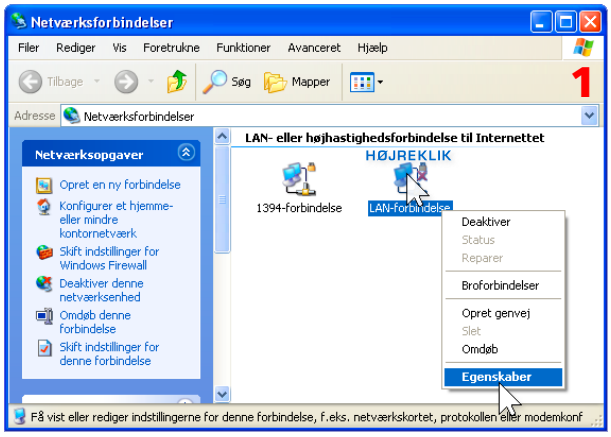


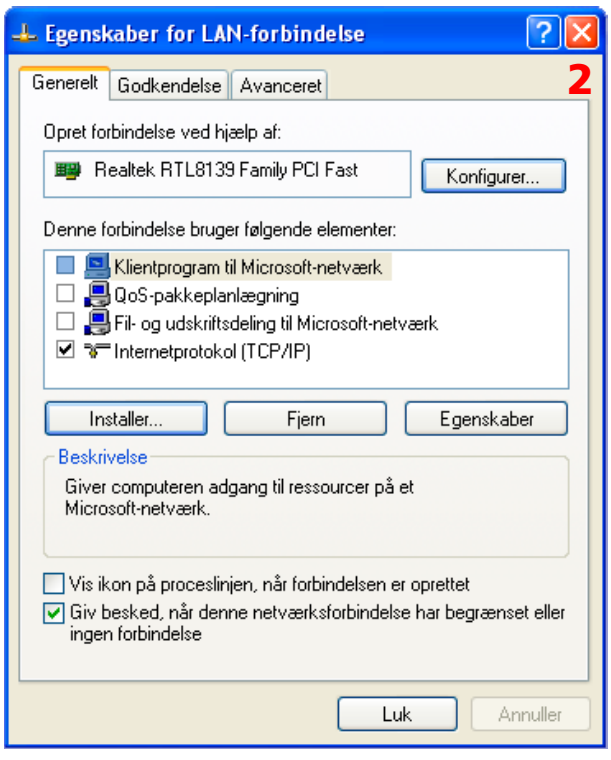
Ved at klikke på Avanceret og derefter WINS-fanebladet, kommer man ind til følgende vindue, hvor NetBIOS skal være koblet til. Derudover skal tjenesten TCP/IP NetBIOS Helper også køre, hvilket den også gør som standard.

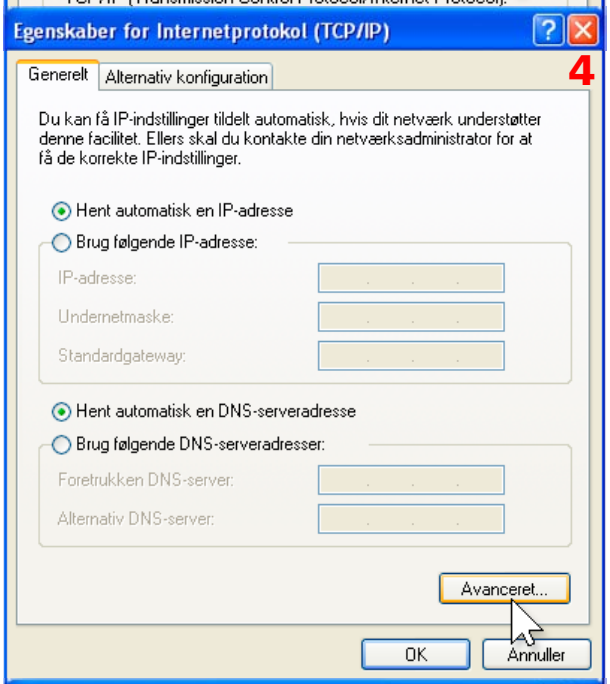


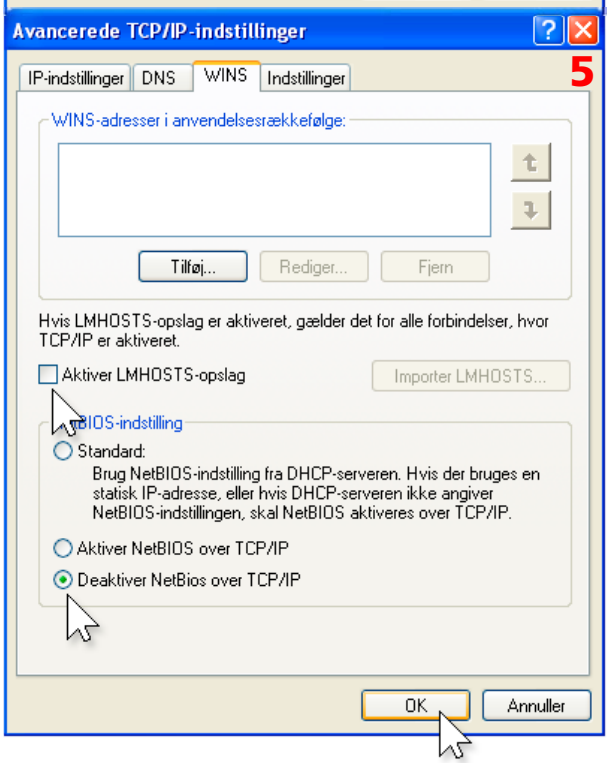
Hvis du ikke har behov for et LAN, kan Klientprogram til Microsoft-netværk, Fil- og udskriftsdeling til Microsoft-netværk samt NetBIOS over TCP/IP kobles fra, for de er ikke nødvendige for at få en enkeltstående computer på internettet. Disse kobles fra inde i Start > Kontrolpanel > Netværks- og Internetforbindelser > 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 Fil- og udskriftsdeling til Microsoft-netværk fjernes og QoS-pakkeplanlægning 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.





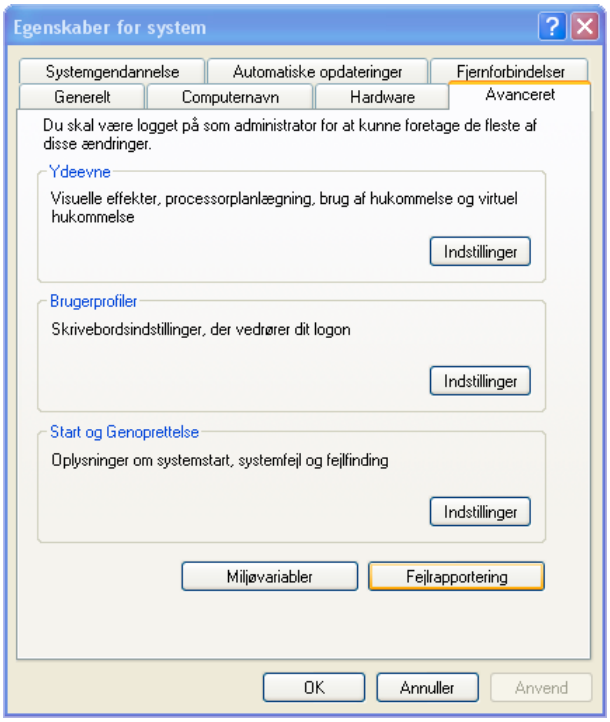




Til sidst vælger jeg at deaktivere tjenester, som godt nok ikke holder en port åben, men som ikke er nødvendige i mit tilfælde og det drejer sig om følgende:

Automatisk konfiguration af trådløse enheder
DNS-klient
Remote Registry
Tjenesten fejlrapportering
Tjenesten TCP/IP NetBIOS Helper (hvis NetBIOS over TCP/IP ikke køres).

Tjenesten fejlrapportering kobler jeg fra, fordi jeg normalt også kobler funktionen Fejlrapportering fra. Den funktion finder man inde i Kontrolpanel > System > Ydelse og vedligeholdelse > Avanceret, som vist herude til højre.



På side 1 deaktiverede jeg Automatiske opdateringer, fordi jeg hellere selv vil opdatere via Windows Update-siden engang imellem. I tidligere versioner af WinXP var tjenesten ved navn Automatiske opdateringer kun nødvendig, hvis man brugte funktionen Automatiske opdateringer, men i SP2 vil Windows Update-siden ikke fungere, hvis tjenesten Automatiske opdateringer ikke kører, så den får lov til at køre her.

Tilbage er der nu kun at besøge Windows Update og få hentet vigtige opdateringer. Det er en god idé at besøge siden ofte.

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.