



Windows XP services forklaret

Windows services kan godt være lidt af en jungle at finde rundt i, Hviske har man brug for, hvilke udgør en sikkerhedsrisiko og hvilke kan med fordel disables? Her er en oversigt. ARTiklen under udarbejdelse

Skrevet den **22. Feb 2009** af **bufferzone** I kategorien **Workstation / Windows XP** | ★★★★★

Nedenstående tabel bør ikke ukritisk betragtes som en facitliste. Du bør tage stilling til hver enkelt service før du beslutter dig om den skal enables eller disables. Tabellen er et udtryk for min personlige holdning, hvor sikkerheden vejer tungt. Følgende generelle betragtninger er anvendt.

- Hvis en service ikke anvendes skal den mindst disables, heldst afinstalleres
- Hvis en services kun anvendes en gang imellem, bør den disables og kun enables i den tid den anvendes

Service bemærkning	Beskrivelse	disable	konsekvens	Råd
Alerter	Udsender administrative alarmer	Ja	Programmer der bruger disse vil ikke modtage nogle alarmer	
Application Layer Gateway	Giver applikations-protokol plug-ins og enabler net-work/protocolconnectivity	Måske	MSN Messenger samt Windows Messenger og lignende programmer vil ikke virke	
Application Managemen	Håndterer installation og removal og enumerations forespørgsler for AD IntelliMirror group policy		IntelliMirror programmer vil ikke kunne bruges	

	programmer		
Automatic	Automatisk down-		Sikkerhedsopdateringer
Kan disables men			
Updates	load og installarion		vil ikke installeres
bør enables, det			
	af kritisk windows	Ja	automatisk, de kan dog
vigtigste er at			
	Sikkerhedsopdate-		installeres manuelt
maskinen er fuldt			
	ringer		
opdateret			
Background	styre dataoverfør-		Ting der kræver data-
Intelligent	sel mellem klient og	Ja	overførsel vil ikke
Transfer	server		virke ordentlig, f.eks
se ovenfor			enable
			windows update
ClipBook	Muliggør at Clip-		Clipboard vieweren kan
	board vieweren kan	Ja	ikke dele indhold med
Disable			
	dele informationer		remote maskiner
	med remote maskiner		
COM+ Event	Tillader management		System Event Notification
System/System	af Component Servi-		vil ikke virke. Logon og
Application	ces via automatisk	nej	logoff notofication vil
			Enable
	distripution af		ikke ske. Andre applika-
	events til abonner-		tioner f.eks Volume Snap-
	ende COM komponenter		Shot Service vil fejle
Computer	Håndterer Browser		Compute4ren kan ikke se
Hvis der skal			
Browser	listen og bruges af		de andre computere på
deles filer og			

	windows programmer	ja	netværket	Enable
ressourcer skal				
	til at se netværks			
denne service				
	domæner & ressourcer			
enables				

Cryptographic	Indeholder følgende:		En meget væsentlig del	
services	Catalog Database		af computerens sikkerhed	
	Service (Fil Signa-		vil ikke fungere ordent-	Enable
	tur), Protected Root		ligt	
	Service (tilføjer og			
	fjerner Trusted Root	Nej		
	Certification Aut-			
	hority certifikater			
	fra computeren) og			
	Key Service (nødven-			
	dig for håndtering			
	af certifikater			

DHCP Client	Håndterer DHCP og		DNS vil ikke virke	
Kan disables hvis				
	Dynamisk DNS	Måske		Enable
DNS ikke bruges				

Distributed	sørger for at gen-		Link tracking vil ikke	
Link Tracking	veje og OLE-links		være til rådighed og andre	
Client	virker selvom target	ja	computere vil ikke kunn	
Disable				
	flyttes eller renam-		tracke links på denne	
	es via links i fil		Computer	
	systemer.			

Distributed	Koordinere transak-		Distripuerede Transak-	
-------------	---------------------	--	------------------------	--

Transaction Coordinator Disable	tioner der spænder over flere ressource managers, f.eks. databaser, message queues og fil systemer ja	tioner vil ikke kunne forekomme	Enable
DNS Client	Opløser og cacher DNS navne. Nødvendig for at DNS fungerer Nej	DNS vil ikke virke Kun IP adresser kan bruges	Enable
Error Reporting Disable	Håndterer fejlrapportering i forbindelse med applikations crash Ja	Kun kernel fejl og visse typer af User Mode fejl vil blive rapporteret	
Event Log	Håndterer event vieweren Nej	Event vieweren vil ikke virke	Enable
Fast User Switching Disable	Håndterer management for applikationer i et domæne der har behov for støtte i et fler-bruger miljø Ja	Fast User Switching vil ikke være til rådighed	
Help and Support Disable	Håndterer hjælp og support i windows Ja	Windows hjælp og support center vil ikke være til	

				rådighed	
HID Input	Håndterer Human			Hot Buttons vil ikke virke	
Nogle keyboards					
	Interface Devices.				
med Hot buttons					
	Aktivere predifine-	Måske			
Disable	vil ikke virke				
	rede Hot Buttons,				
	Remote controles og				
	andre multimedia				
	devices				
IMAPI CD-	Håndtere CD brænding			CD brænder vil ikke virke	
Disable hvis der					
Burning COM	med Image Mastering	Måske			Enable
ikke findes en CD					
	Applications Program				
brænder					
	ming Interface				
Indexing	Indexere indhold og			Filer vil ikke blive	
Denne service bør					
Service	properties af filer	ja		indexseret	
Disable	afinstalleres				
	på lokale og remote				
hvis den ikke					
	computere				
bruges					
Internet	Håndterer network			Internet sharing, name	
Installer en					
Connection -	address translation			resolution og firewall	
anden firewall					
Firewall(ICF)	(NAT), Navne opløs-	Måske		vil ikke virke	
Disable	denne er ikke				
Sharing(ICS)	ning og intrusion				
god nok					
	prevention services				
IPSEC	Håndterer IPsec			IPsec baseret VPN vil	
Hvis du bruger					
services	support til VPN	Måske		ikke virke	

Disable SEC baseret VPN				
så enable denne				
Logical Disk Håndterer dynamiske		Nytilsluttede diske vil		
Kan sagtens dis-				
Manager disk informationer		ikke automatisk blive		
ables hvis du				
	tilsluttes nye diske ja	opdaget af windows	enable	
forventer at til-				
	sendes nødvendige			
flere nye diske				
	data til LDM admini-			
	strative service			
Logical Disk Håndterer disk og		Startes automatisk når		
Disable hvis oven				
Manager partitions konfigura Ja		der er behov derfor	Måske	
stående service				
Administrative tion af nye diske				
service				
Machine Håndterer Visual		Visual Studio debugging		
Debug Studio debugging Ja		vil ikke virke		
Disable				
Manager				
Messenger Håndterer Alerter		Net send vil ikke virke		
Har inter med				
	service og net send Ja			
Disable Messenger at gøre				
	beskeder mellem			
	server og klienter			
Microsoft Håndterer software-		volume shadow copies vil		
Disable hvis du				
Software baseret shadow Ja		ikke virke		
Disable ikke ønsker at				
Shadow Copy copies af Volume				
anvende Shadow				
Provider Shadow Copy service				
copies				

NetMeeting	Tilader en autorise-		Remote Desktop sharing	
NetMeeting udgør				
Remote	ret bruger at tilgå	Ja	via NetMeeting vil ikke	
Disable	en sikkerheds-			
Desktop	computeren remotely		virke	
risiko				
Sharing	via NetMeeting			
Network	Håndterer dial-up		Network konfiguration	
Connections	connections for		vil ikke virke, Andre	Enable
	servere herunder	Nej	services vil også fejle	
	network status noti-			
	fication og konfigu-			
	ration			
Network DDE	Håndterer network		DDE transport og sikkerhed	
	transport og sikker-		vil ikke virke	
Disable	hed for Dynamic Data	Ja		
	Exchange (DDE)			
Network DDE	Håndterer Dynamic		DDE Network shares vil	
DSDM	Data Exchange (DDE)	Ja	ikke virke	
Disable	network shares			
Network	En del af ICS		ICF og ICS vil ikke virke	
Enable hvis ICF				
Location	Håndtere konfigura-			
Disable	bruges			
Awareness	tions- og placerings	Måske		
(NLA)	oplysninger			
NT LM	Håndterer NT 4.0		NT 4.0 klienter vil ikke	

bør kun enables			
Security	(pre win 2000) logon	Disable	kunne logge på
disable	hvis NT 4.0 klien		
Support			
ter skal logge på			
Provider			
Performance	Håndterer logging og		Performance data vil ikke
Logs and	Displaing af perfor	Ja	blive logget
Disable			
Alerts	mance data		
Plug and Play	Håndterer Plug and		Plug and Play vil ikke
	Play	Nej	virke
			Enable
Portable	Håndterer serienumre		beskyttet materiale vil
Media Serial	til externe media	Ja	ikke altid kunne
downloade	Disable		
Number	players		
Print Spooler	Håndterer print jobs		man vil ikke kunne printe
Kan disables			
	og network print	Nej	
hvis maskinen			Enable
	queues		
ikke skal printe			
Protected	Håndtere beskyttelse		De beskyttede informatio-
Storage	af følsomme informa-	Ja	ner vil være utilgængelige
	tioner, f.eks.		lige
	private keys		
QoS RSVP	Håndterer network		QoS-aware applikationer
	signaling, trafik	ja	vil ikke virke ordentligt
Disable			
	kontrol og setup for		

	QoS-aware applikatio-		
	ner		
Remote Access	Håndterer remote		brugere må connecte
Auto Connection	access. Finder al-	Ja	manuelt til andre systemer
Manager	ternativer ved mis-		
	lykkedes connection		
	forsøg		
Remote Access	Håndterer Dial-up og		Operativsystemet fungere
Startes On-Demand			
Connection	VPN forbindelser	Måske	ikke ordentligt
af Remote Access			
Manager			
Manager			
Remote Desktop	Håndterer Remote		Remote Assistance vil ikke
Help Session	Assistance	Ja	virke
Disable			
Manager			
Remote	håndterer RPC name		Flere OS komponenter vil
Procedure	service	Nej	ikke fungere ordentligt
Call (RPC)			Exchange og andre tredie-
			parts utils vil ikke virke
Remote	Håndterer remote		Hfnetchk, patch utility
Registry bør ikke			
Registry	management af system	Ja	og tilsvarende applikatio-
Disable kunne tilgås	registry		ner vil ikke virke
remote. Enable			
ved behov			
Removable	Håndterer flytbare		applikationer og systemer

Enable hvis flyt			
Storage medier og automatisk Ja der bruger flytbare			
medier Disable medier anvendes			
afbrydelse af disse		vil virke langsomt	
Routing og Håndterer multiproto		Routing og Remote Access	
Undlad at instal			
Remote kol LAN-to-LAN, LAN- Ja vil ikke virke			
Disable lere denne servi			
Access to-WAN, VPN og NAT			
ce vil muligt			
routing services			
Secondary Håndterer "RUN AS" Ja Run AS vil ikke virke			
Disable Enable ved behov			
Logon			
Security Håndterer account		services der kræver ad-	
Hvis DHCP ikke			
Accounts informationer for		gang til SAM vil ikke	
anvendes kan den-			
Manager de lokale security Ja virke. F.eks. GPO Enable			
ne service dis-			
accounts og dermed		kan fejle	
ables			
services afgang til			
SAM			
Server Håndterer fil og		Fil og print, RPC	
Enable hvis du			
print deling samt Ja requests samt pipe			
Disable fil deler			
pipe communication		kommunikation vil ikke	
		virke	
Shell Hardware Håndterer notifika		CD-rom og andre devices	
Detection tion for AutoPlay Ja vil ikke virke Enable			
hardware events		automatisk	

Smart Card	Håndterer adgang til		Smart Cards vil ikke kunne
Enable hvis smart			
	smart Cards	Ja	læses
Disable Cards anvendes			

Smart Card	Håndterer adgang til		Ældre smart Cards vil
Helper	ældre Smart Cards	Ja	ikke kunne læses
Disable			

SSDP	Håndterer sammen med		UPnP devices vil ikke
Discovery	Universal Plug and	Ja	virks
Disable			
	Play Device Host		
	UPnP devices		

System Event	Håndterer Event Log		Notificering og
Bærbare kan			
Notification	notificere COM+ sub-	Ja	synchronisering vil
Disable enable	denne		
	scribers om Logon og		virke
	power-relaterede		
	events		

System Restore	Håndterer system		Automatisk system gendan-
Enable hvis der			
	restore herunder	Ja	nelse vil ikke virke
Disable ændres	meget ved		
	genskabelses punkter		
systemet			

Task Scheduler	Håndterer schedule-		schedulering vil ikke
Enable kun ved			
	ring af opgaver	Ja	virke
Disable behov			

TCP/IP NetBIOS	Håndterer NetBIOS		NetBIOS over TCP/IP
Enable kun ved			
Helper	over TCP/IP og		samt deling af ressourcer
Disable ved behov			
	NetBIOS name lookups	Ja	vil ikke virke

	bruges af GPO			
	software distribu.			
Telephony	Håndterer Telephony		TAPI applikationer vil	
	API (TAPI) herunder	Ja	virke dårligt	
Disable				
	IP-based voice			
Telnet	Håndtere TelNet	Ja	TelNet vil ikke virke	
Disable				
Terminal	Håndterer windows		Terminal services	
Services	Terminal. bruges af		vil ikke virke	
	Remote Desktop, Fast	Ja		
Disable				
	User Switching, Re-			
	mote Assistance og			
	Terminal Server			
Themes	Håndterer theme		theme kan ikke bruges	
Disable				
	Management	Ja		
Uninterruptibl	Håndterer UPS manage		UPS management kan	
e Power Supply	ment	Ja	ikke gennemføres	
Disable				
Universal Plug	Bruges sammen med		uPnP devices kan ikke	
and Play Device	SSDP Discovery ser-	Ja	findes på nettet	
Disable				
Host	vice			
Upload Manager	Håndterer synchro		Nogle former for fil	
	og asynkron fil-	Ja	overførsel vil ikke	

Disable			
	overførsel		virke
Volume Shadow	Håndterer Volume		Shadow copies vil ikke
Copy	shadow copies	Ja	virke
Disable			
WebClient	Giver Windows-base-		Web baserede filer kan
	rede programmer		ikke tilgås
	mulighed for at op-	Ja	
Disable	rette, tilgå og mo-		
	dificere web base-		
	rede filer		
Windows Audio	Håndterer audio		Audio devices vil ikke
	devices	Ja	virke ordentligt
Disable			
Windows Image	Håndterer billed		Billedoverførsel vil
enable hvis			
Acquisition(WIA)	overførsel fra kame-	Ja	ikke virke
Disable kamera eller scan-			
	raer og scannere		
ner anvendes			
Windows	Håndterer MSI		Installerer vil give
Installer	pakker	Ja	problemer
			Enable
Windows Manage-	Håndterer system		performance alerts vil
ment Instrumen-	management informa-		ikke virke
tation (WMI)	tion. Bruges til	Nej	
			Enable
	implementering af		
	performance alerts		

WMI Driver	Håndterer alle drev		extension til WMI	
Extensions	og event trace pro-		virker ikke	
	viders konfigureret	Ja		Enable
	til WMI eller event			
	trace information			
Windows Time	Bruger NTP til tids		NTP vil ikke virke	
Brug altid NTP i	synchronisering	Ja		Enable
et netværk miljø				
Wireless Zero	Wifi Plug'n Play	Ja	Wifi plug'n play vil ikke	
Enable hvis Wifi				
Configuration			virke	
Disable	anvendes			
WMI Performance	Håndtererere perfor-		startes når Per-	
Adapter	mance library in-	Ja	formance Data	Enable
	formation fra VMI		Helper startes	
Workstation	Håndterer Microsoft		Computeren vil ikke kunne	
	Network services	Ja	tilgå netværks ressourcer	Enable

Tillæg til denne artikel kan findes gratis her

<http://www.eksperten.dk/artikler/737>

Kommentare og forslag modtages som sædvaneligt med kyshånd. Spørgsmål er også velkomne, både på eksperten og på kim@bufferzone.dk. Undlad venligst at stille spørgsmål i artiklens kommentare, dem kan jeg jo ikke besvare

En OK liste, men det bør fremgå at navnene er taget fra en engelsk WinXP, og du bør efter min mening bestemme dig for om du vil holde dig til engelske eller dansk udtryk i artiklen - det er ikke så kønt at blande det hele sammen. Du bør desuden selv gennemlæse artiklen og/eller køre en stavekontrol på den da der er mange stave- / tastefejl.

Kommentar af nanoq d. 15. Aug 2005 | 2

En god og nyttig artikel.

Jeg forstår ikke, hvorfor wickedd giver dårlig karakter, for en så god og nyttig information. At artiklen ligner noget der allerede eksisterer, er da ligegyldigt. Faktisk vil langt størsteparten af artikler på Eksperten, ligne noget der eksisterer i forvejen, alene i kraft af det ENORME antal artikler der findes på internettet.

Kommentar af lenk d. 05. Aug 2005 | 3

Endnu en nyttig artikel som XP brugere bør kikke på. Selvom man kan negelsk, er fagsproget når man taler om services ofte lidt svært, det letter det hele en del at det er på dansk

Kommentar af barbarbo d. 02. Aug 2005 | 4

Dejligt med en brugbar oversigt på dansk og med tillæget har man faktisk mulighed for at styre sine services som man ønsker. At skemaet ligner andre på nettet er vel ganske naturligt, det er jo de samme services der er tale om så det kan vel ikke være meget anderledes

Kommentar af serverservice d. 21. Apr 2006 | 5

Der er en del services man lige bør overveje om de bør disables.
Alerter, Netbios, Logical disk management, System event notification oa.
Artiklen virker lidt nem og ikke så gennearbejdet som normalt fra bufferzone.

Kommentar af wickedd d. 27. Jul 2005 | 6

Ligner den her lidt for meget: <http://www.majorgeeks.com/page.php?id=12>

Kommentar af wollsen (nedlagt brugerprofil) d. 09. Nov 2005 | 7

nice, god og nyttig info!

Kommentar af jensen5 d. 31. Jul 2005 | 8

Kommentar af michaelthr d. 03. Nov 2005 | 9