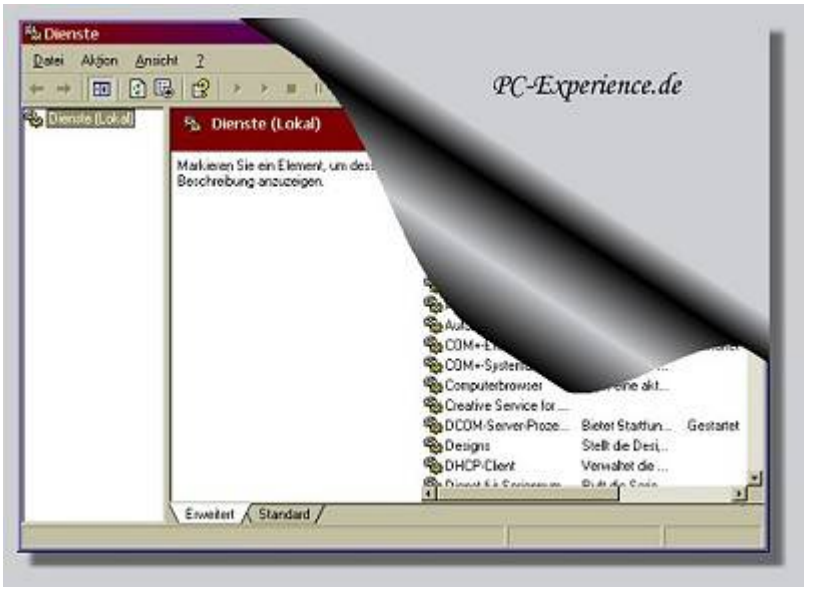
Windows 2000/XP - Diensteoptimierung -Workaround-

- Update 06.2008 -



Einleitung

Wie definiert man die Bedeutung eines Dienstes unter einem NT-Betriebssystem?

"Als Vorgang einer algorithmisch ablaufenden Informationsverarbeitung im Kontext eines Betriebssystems".

Klingt doch etwas verwirrend nicht wahr?
Mit diesem Artikel möchten wir die Definition der Dienste unter Windows 2000/XP nicht nur näher erläutern, sondern vor allem auf die einzelnen Funktionen und Aufgaben eines Dienstes im Zusammenhang mit dem Betriebssystem eingehen. Mögliche und vor allem sinnvolle Optimierungen haben wir dabei berücksichtigt.

Die Windows-Dienste sind von zentraler Bedeutung für die Funktionsweise des Betriebssystems und der geladenen Programme. Zahlreiche Dienste werden vom System verwaltet und funktionell gesteuert. Dadurch werden Aktionen ermöglicht, wie beispielsweise das Anmelden am Betriebssystem, Datei- und Druckfunktionalität und natürlich auch die vielfältige Unterstützung in Netzwerken. Unter Windows 2000 und XP starten viele Komponenten des Betriebssystems als Dienst und die meisten davon sind für eine reibungslose Arbeit von Windows zwingend notwendig. Jedoch sind Dienste auch die Hauptangriffsfläche für Angreifer von außen, welche Berechtigungen und Funktionen eines Dienstes ausnutzen, um Zugriff auf eine lokale Arbeitsstation oder einen Server in unserem Netzwerk zu erhalten. Und damit stellen Dienste, vor allem die, die mit überflüssigen Berechtigungen ausgeführt werden, ein besonderes Sicherheitsrisiko dar. Abgesehen von den für den reibungslosen Ablauf des Betriebssystems notwendigen Diensten, sollten wir nicht benötigte Dienste deaktivieren. Damit dezimieren wir nicht nur eine Angriffsfläche, sondern erreichen auch einen leichten Performancegewinn, denn ein aktivierter und gestarteter Dienst läuft permanent im Hintergrund, unabhängig davon, ob wir den Dienst tatsächlich benötigen. Dieser Zustand belastet mitunter

unnötigerweise unsere Systemressourcen.
Im Vordergrund unserer Bemühungen stehen aber ganz klar die Zugewinne an Sicherheit, die nicht von der Hand zuweisen sind.
All dies ereichen wir, indem wir nicht benötigte und gefärliche Dienste deaktivieren oder deren Autostartyp ändern. Hierbei ist jedoch höchste Vorsicht geboten, denn ein deaktivierter Dienst, der von einer Anwendung benötigt wird, wird nicht nur zu Fehlermeldungen führen, sondern auch die Gesamtfunktion des Programms verweigern, das ist definitiv nicht unser Ziel.

Definition von Diensten

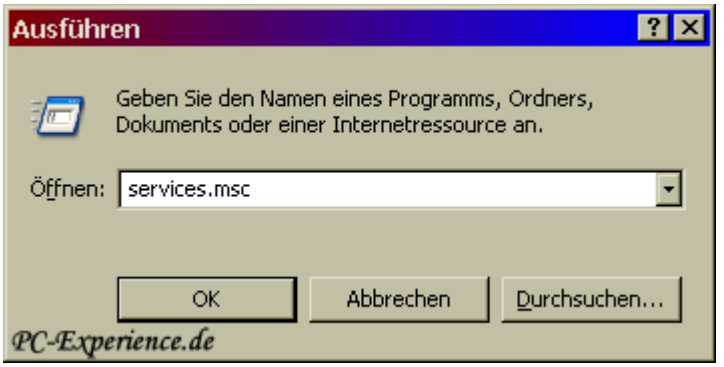
Befassen wir uns vorab mit dem grundlegenden Dienstemodell, worauf die Windows NT-Architektur basiert. Dieses Modell umfasst Einzelmodule, die bestimmte Systemfunktionen einschließen. Viele Dienste stehen in Abhängigkeit zu anderen Diensten, eine Tatsache, die unser Augenmerk umso mehr schärfen sollte, wenn es darum geht, einen Dienst (auch als Prozess bezeichnet) abzuschalten oder gar zur Gänze zu deaktivieren. Ein Dienst bildet das Kernstück des Betriebssystem-Dienstcontrollers. Hierbei handelt es sich um die Datei Services.exe, die wir im Verzeichnis \winnt\system32 finden. Im „Windows Task-Manager" auf der Registerkarte „Prozesse" werden uns alle aktuell ausgeführten Dienste angezeigt. Abgesehen von den Systemdiensten, kann ein Dienst aber auch Teil eines Programms oder eine speziell benötigte Funktion einer Serveranwendung darstellen. Dienste werden auch durch sicherheitsrelevante Programme wie Desktop-Firewalls und Antivirenwächter gestartet, leider nutzen aber auch diverse Spionageprogramme und Viren diesen Weg, um sich bei jedem Start sofort in das System zu integrieren. Also Augen auf bei verdächtigen Aktionen eures Systems!

Diensteverwaltung

Die Betriebssysteme Windows 2000 und XP bieten uns eine komfortable Verwaltungsoberfläche in Form der „Microsoft Management Console", kurz und bündig MMC genannt. Bereits mit der Installation unseres Betriebssystems werden eine Menge an vorgefertigter MMCs für den administrativen Bedarf bereitgestellt. Für den Handwerker ist der gute Schraubendreher im Werkzeugkoffer unverzichtbar, in einer MMC wird ein Werkzeug als „Snap-In" bezeichnet. Und auch hier zählt die Anforderung, je nachdem wird die MMC mit unterschiedlichsten Snap Ins ausgestattet sein.

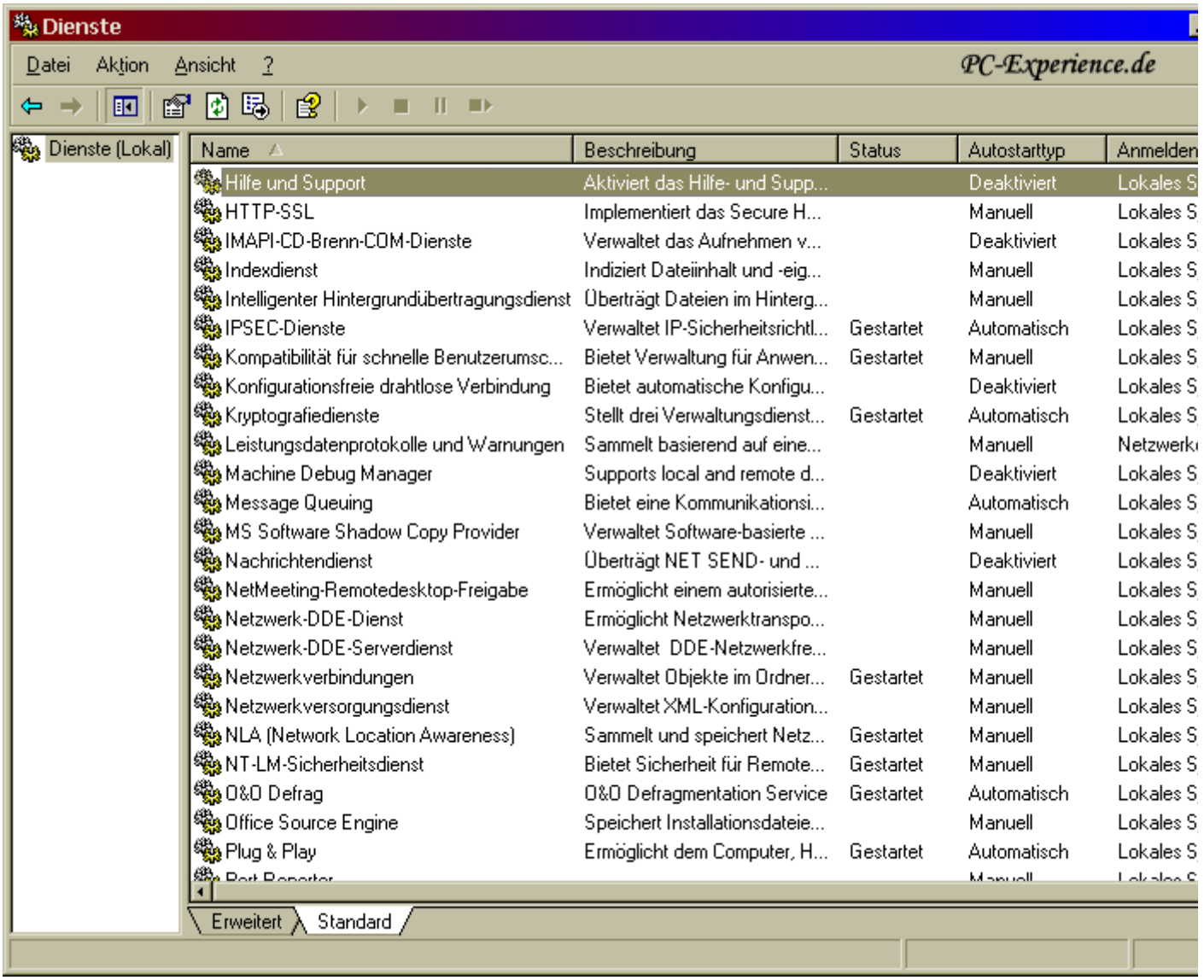
Die MMC „Computerverwaltung", welche wir über die Systemsteuerung -> Verwaltung aufrufen können, sei hier als Beispiel genannt. In dieser MMC befindet sich unter anderem auch das Snap-In zur Diensteverwaltung. Dieses können wir aber auch solo starten:

Start –> Einstellungen -> Systemsteuerung -> Verwaltung -> *Dienste*
Alternativ bietet sich der Aufruf über Start - > Ausführen an.
In das Ausführen-Feld geben wir den Befehl services.msc ein und bestätigen diese Eingabe mit dem Button OK oder durch Drücken der ENTER-Taste (.msc steht für die Dateiendung einer MMC)



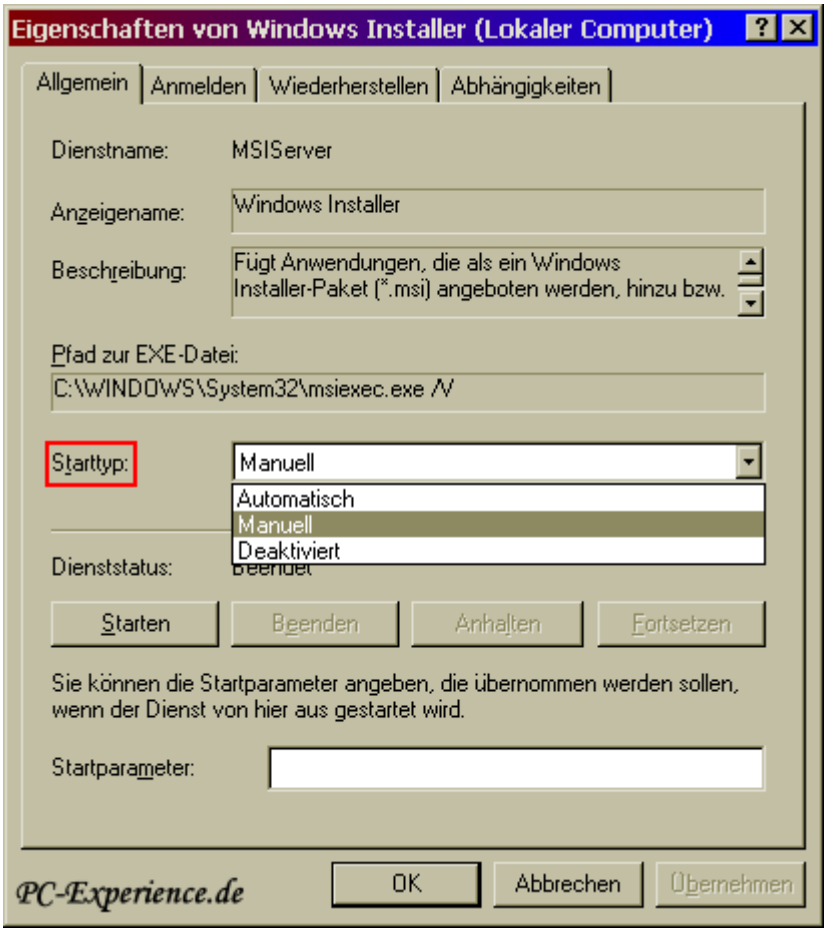
Standardmäßig finden wir im rechten Bereich des Dienstefensters 5 Spalten mit Informationen zu jedem aktuell installiertem Dienst. Diese Ansicht erhalten wir nur, wenn über das Menü "Ansicht" in der obigen Symbolleiste die Details eingeblendet werden.

Name: der vollständige Dienstname wird angezeigt.
Beschreibung: die Funktion des Dienstes.
Status: der aktuelle Zustand des Dienstes.
Autostarttyp: beschreibt das Verhalten des Dienstes beim Systemstart.
Anmelden als: zeigt an, über welches Konto der Dienst angemeldet wurde.



1. Allgemeine Eigenschaften eines Dienstes

Um die Eigenschaften eines Dienstes im Detail betrachten zu können, führen wir direkt auf dem Dienstnamen einen Doppelklick aus und wir landen im Eigenschaftsfenster.



In der ersten Registerkarte „Allgemein“ finden wir eine Menge an Informationen zu dem jeweiligen Dienst:

- Der Dienstname wird vollständig im Original angezeigt, in unserem Beispiel lautet der Name: „MSIServer“. Das Format des Dienstnamens entspricht auch dem vieler Befehlszeilenprogramme.
- Der Anzeigename, der auch gleichzeitig in der Übersicht des Dienstehauptfensters angezeigt wird, und diesen Dienst als „Windows Installer“ präsentiert.
- Die Beschreibung erklärt uns kurz und bündig die Funktion des Dienstes. Diese ist im Hauptfenster über die Ansicht „Erweitert“, auf die wir im unteren Bereich des Fensters umschalten können, aber besser einzusehen.
- Eine wesentliche Info gibt uns der Pfad zur EXE-Datei an. Damit können wir den Standort des Dienstes, wie auch den dazugehörigen Dateinamen und etwaiger Parameter lokalisieren. Der Pfad und der Dateiname des Dienstes können nicht verändert werden. Wenden wir uns nun einem sehr wichtigen Punkt zu, dem Startverhalten eines Dienstes.

Die Starttypen:

Wir unterscheiden drei Starttypen der Dienste unter Windows:

- Automatisch - Der Dienst wird automatisch beim Starten des Betriebssystems geladen und ausgeführt. Ganz unabhängig davon, ob dieser auch tatsächlich benötigt wird.

- Deaktiviert - Der Dienst wird beim Starten des Betriebssystems nicht geladen. Dienste, die von dem nicht gestarteten Dienst abhängig sind, werden ebenfalls nicht gestartet. Dieser Umstand kann

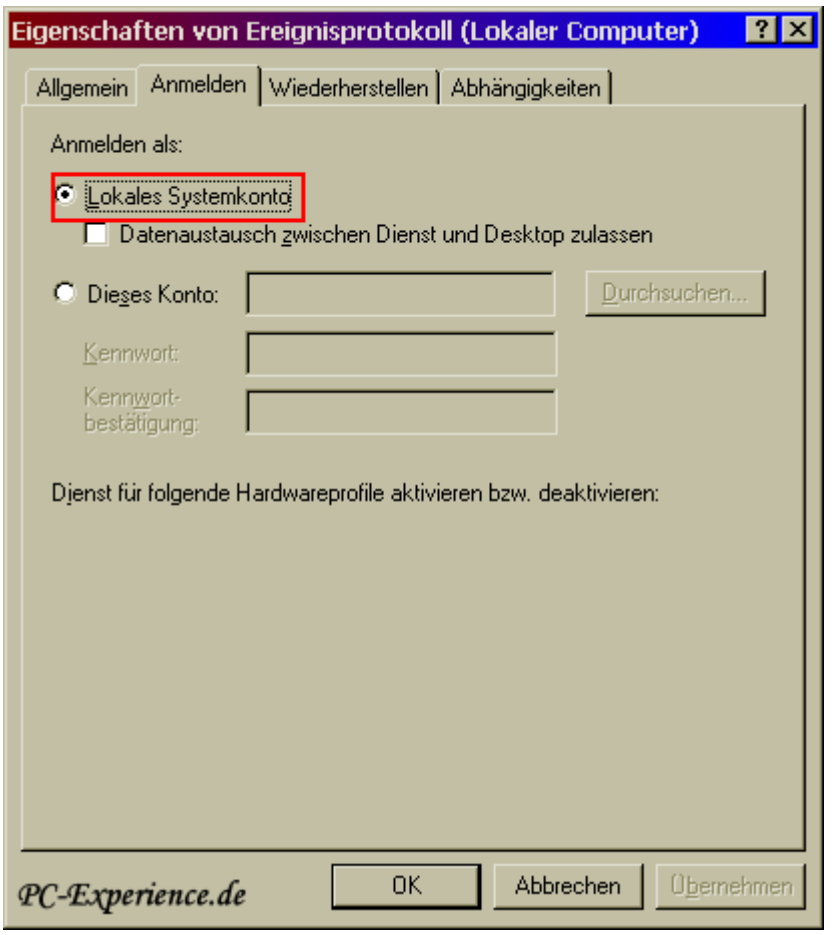
zu Problemen führen, also Achtung beim Deaktivieren eines Dienstes.

- Manuell – Auch mit dieser Einstellung wird der Dienst beim Starten des Systems nicht geladen. Entweder müssen wir den benötigten Dienst manuell über die Konsole "Dienste" starten, oder ein Programm fordert den Start eines ihm zugehörigen Dienstes selbst an. Im Feld „Startparameter", können eventuell benötigte Parameter eingetragen werden, die beim Starten des Dienstes von hier aus beachtet werden sollen. Diese Einstellungen werden im Bedarfsfall nur einmal ausgeführt und nicht dauerhaft gespeichert.

Die Anmeldung eines Dienstes:

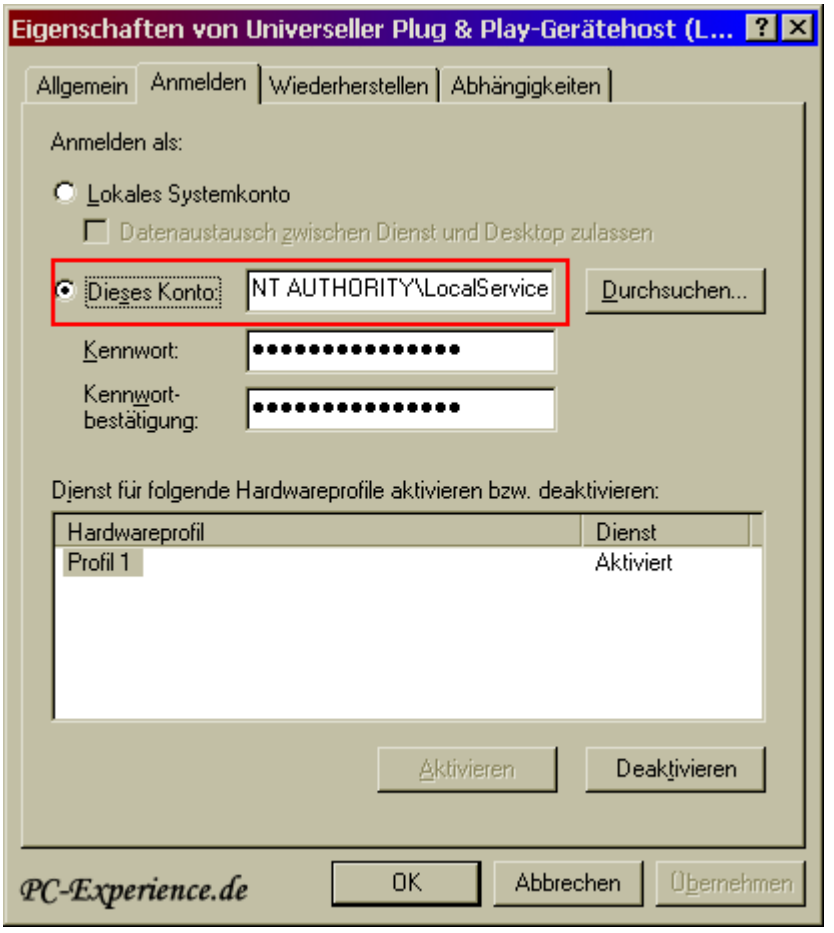
Ein Dienst muss über ein Konto angemeldet sein, damit dieser auch auf Ressourcen und Objekte des Betriebssystems zugreifen kann. Wir unterscheiden hierbei aber ganz klar zwischen einem Systemkonto und dem uns üblich bekanntem Benutzerkonto, welches wir nach dem Start des Betriebssystems für unsere Benutzeranmeldung verwenden. Die meisten Dienste melden sich über das Systemkonto an, unabhängig von einem manuellen Eingriff unsererseits. Diese Standardeinstellung sollten wir nicht unüberlegt ändern, denn es kann durchaus sein, dass sich ein Dienst unter Verwendung eines geänderten Kontos nicht mehr starten lässt.

- Das lokale Systemkonto verfügt über Vollzugriff auf das System. Der Name des lokalen Systemkontos ist LocalSystem.

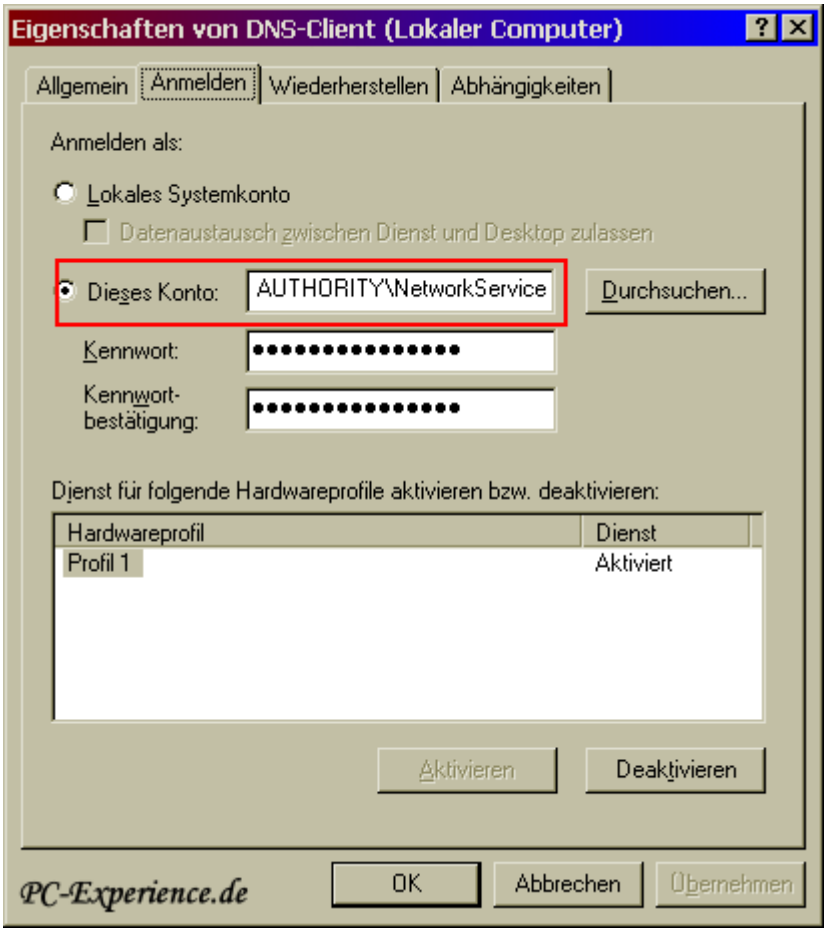


- Das lokale Dienstkonto ist ein spezielles Konto, das einem authentifizierten Benutzerkonto ähnelt.

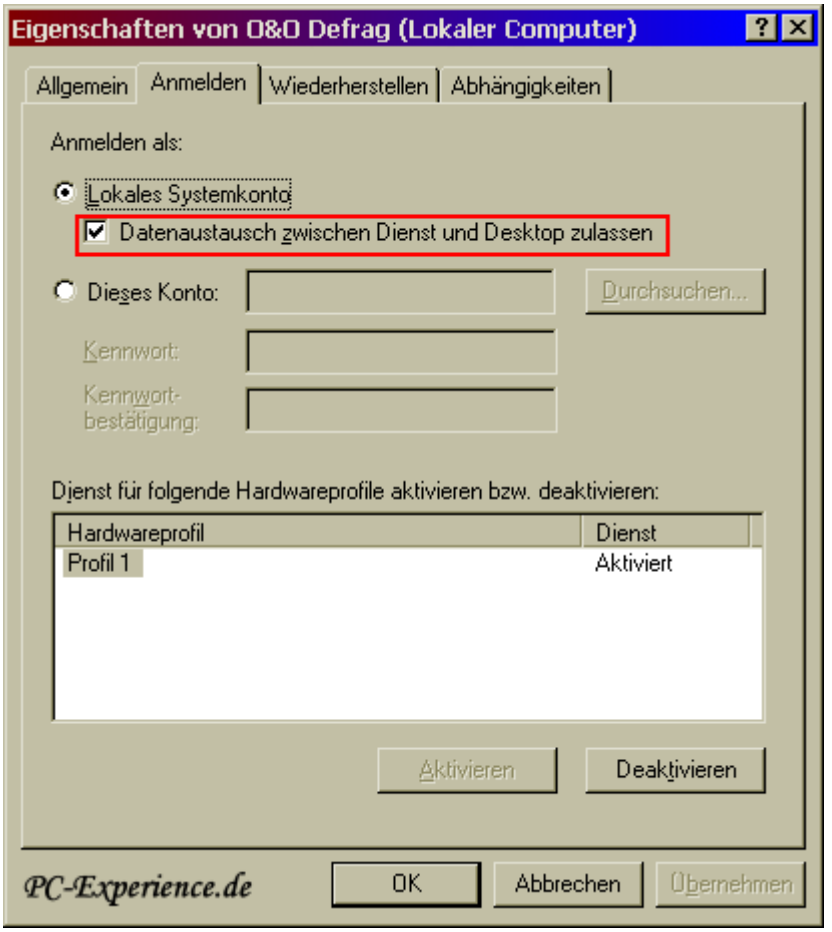
Dieses Konto verfügt über dieselben Zugriffsrechte auf Ressourcen und Objekte wie die Mitglieder der vordefinierten Gruppe „Benutzer“ (eingeschränkter Benutzer). Der Vorteil liegt darin, dass durch diesen eingeschränkten Zugriff das System geschützt wird, wenn einzelne Dienste gefährdet sein sollten. Dienste, die über das lokale Dienstkonto ausgeführt werden, greifen auf Netzwerkressourcen mit anonymen Anmeldeinformationen zu. Der Name des lokalen Dienstkontos lautet NT-AUTORITÄT\LocalService.



- Das Netzwerkdienstkonto ähnelt ebenfalls einem authentifizierten Benutzerkonto und verfügt über dieselben Zugriffsrechte wie das lokale Dienstkonto. Auch hier wirkt der Systemschutz durch die Einschränkung im Falle einer Gefährdung. Jedoch greifen Dienste, die über dieses Konto ausgeführt werden, auf die Anmeldeinformationen des Computerkontos auf Netzwerkressorucen zu. Ein Computerkonto ist beispielsweise in einer Domäne als Mitgliedscomputer registriert. Der Name des Netzwerkdienstkontos ist NT-AUTORITÄT\NetworkService.



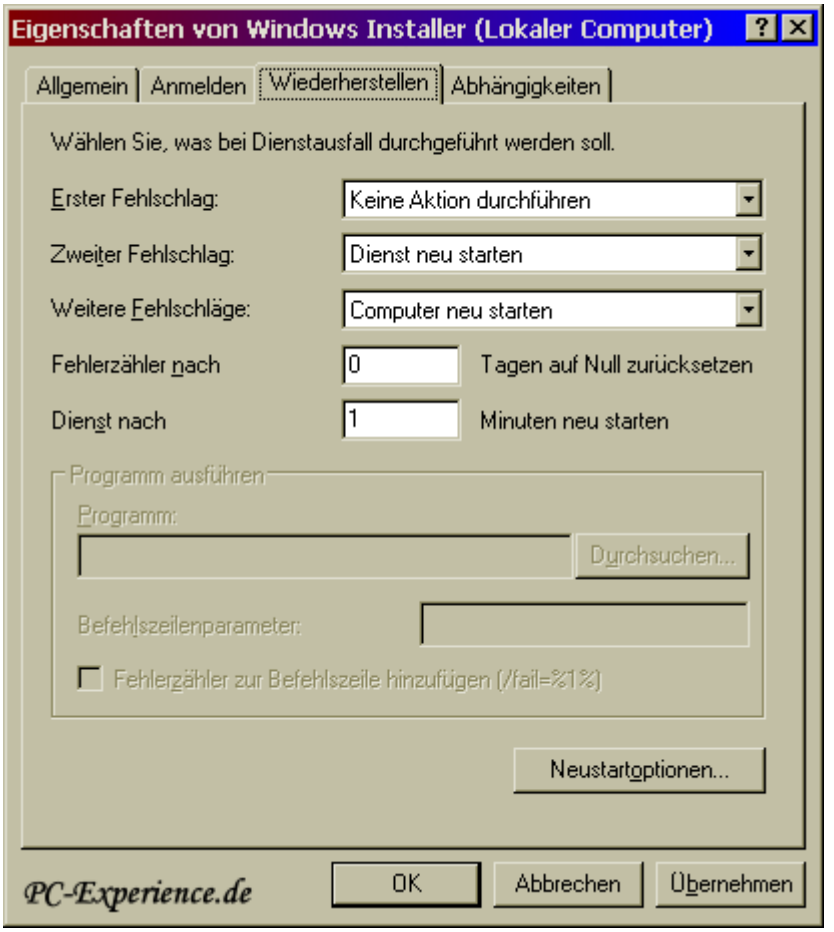
- Im Register „Anmelden“ sehen wir auch die Checkbox „Datenaustausch zwischen Dienst und Desktop zulassen“. Anhand unseres Beispiels mit dem Dienst des Programms "O&O Defrag" wird durch Aktivierung dieser Checkbox angegeben, ob der Dienst auf dem Desktop eine Benutzeroberfläche anzeigt, welche von jedem Benutzer verwendet werden kann, der beim Start dieses Dienstes angemeldet ist und über die benötigten Rechte verfügt. Diese Option ist allerdings nur dann verfügbar, wenn der Dienst über das lokale Systemkonto ausgeführt wird.



Achtung: beide Konten existieren nur bei Windows XP und 2003 Server (NT-AUTORITÄT\LocalService und NT-AUTORITÄT\NetworkService) !

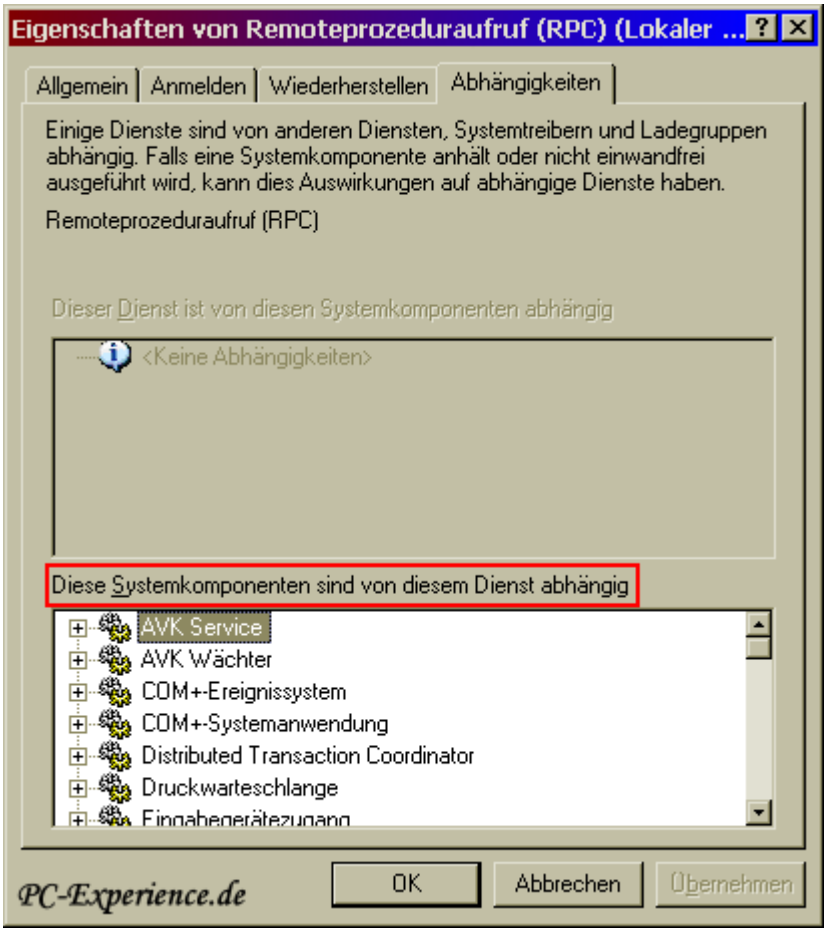
Wiederherstellen bei Dienstausfall:

Sollte ein Dienst während des laufenden Betriebes ausfallen, können wir in diesem Bereich mittels Drop-Down-Listen das Verhalten des Dienstes respektive des Systems je nach Anzahl der Fehlschläge beeinflussen. Unsere Beispielseinstellungen sind selbsterklärend und nach eigenem Ermessen vorzunehmen. Über den Button „Neustartoptionen" unten rechts, könnt ihr angeben, nach wie vielen Minuten der Computer neu gestartet werden soll, sowie auch eine Nachricht an andere Computer im Netzwerk versenden. Vorausgesetzt, dass für diesen Bedarf ein Netzwerk vorhanden, und der Nachrichtendienst aktiviert ist.



Dienstabhängigkeiten:

Viele Dienste stehen in direkter Abhängigkeit zueinander und damit auch die Funktionsfähigkeit. In unserem Beispiel wird angezeigt, dass der Dienst „Remoteprozeduraufruf (RPC)“ in vielerlei Abhängigkeiten zu anderen Diensten steht. Es wäre fatal diesen Dienst zu beenden oder gar zu deaktivieren, da alle damit verbundenen Dienste ebenso nicht mehr funktionieren würden, bishin zum totalen Systemcrash. Wir sehen, dass viele Komponenten vom gestarteten RPC Dienst abhängig sind, dieser selbst jedoch in keiner Abhängigkeit zu einem anderen Dienst steht.



2. Diensteoptimierung und Konfiguration

Windows 2000 und XP gehen mit Diensten im Standard sehr üppig zur Sache. Nicht alle Dienste werden von uns im Status „gestartet“ benötigt. Der uns bereits bekannte Taskmanager eignet sich sehr gut, um die laufenden Prozesse, ob vom Systemkernel selbst oder vom Benutzer angefordert, einzusehen. Die Speicherauslastung wird damit ersichtlich, denn jeder gestartete Dienst, ob nun benötigt oder nicht, ist im Speicher aktiv und belastet somit unsere Systemressourcen.
Der Bedarf ist nicht nur vom System selbst abhängig, sondern auch von unseren eigenen Anforderungen und Arbeitsumgebungen. Die Dienstekonfiguration wird sich von einen Einzelplatzrechner gegenüber einer Netzwerkumgebung und Serverzusatzdiensten immer unterscheiden. Diese wesentlichen Kriterien müssen wir vorab genauestens abwägen, die Beschreibungen zu den einzelnen Diensten lesen und vor allem die Abhängigkeiten der Dienste untereinander berücksichtigen. Erst danach macht eine Konfiguration zur Optimierung auch Sinn, wir möchten ja ein stabiles System beibehalten. Wenn wir für unseren Eigenbedarf unnötige Dienste deaktivieren, erreichen wir auch einen Performancezuwachs für unser System. Zudem schließen wir damit einige Sicherheitsrisiken aus. Die optimale Übersicht der Dienste und deren Status bietet uns das Dienstehauptfenster, welches wir bereits kennen gelernt haben.

3. Die Konfiguration der Dienste

Folgende Elemente listen wir bei den nachstehenden Diensten auf:

- Den Anzeigenamen des Dienstes

- Die Sternchennotiz ** hinter dem Dienstnamen weist auf eine Änderung von Windows XP SP 1a zu Windows XP SP 2 hin! Diese Änderungen betreffen entweder den Anzeigenamen oder die Standardeinstellung des Dienstes. Der Hinweis kann aber auch für einen gänzlichen neuen Dienst, der erst ab SP 2 verfügbar wurde gelten.

- Eine kurze Erklärung zum jeweiligen Dienst soll uns die Funktion verständlich näher bringen.
- Standard: diese Einstellung finden wir unmittelbar nach der Basisinstallation des Systems vor.
- Empfehlung: Für eine sichere Konfiguration, die nicht zu aggressiv in das System eingrifft.
- System: Windows XP verfügt über mehr Dienste als Windows 2000, speziell nach SP 2. Von daher kann die Diensteauflistung je nach System, Servicepackstand und Eigenbedarf variieren.
- Konsequenz bei deaktiviertem Dienst: wir weisen speziell bei wichtigen Systemdiensten explizit auf die Folgen bei „Deaktivierung" hin.

Spezielle Dienste für Serverbetriebssysteme werden nicht berücksichtigt, das würde den Rahmen dieses Workarounds sprengen. Zudem hängen serverspezifische Dienste von der individuell gegebenen Netzwerkumgebung ab.

Vor der Dienstekonfiguration zu beachten!

1. Wir notieren uns die aktuellen Diensteinstellungen, indem wir eine Liste aus dem Dienstehauptfenster exportieren. Das geht sehr einfach über die Menüfunktion *„Liste exportieren"*. Diese Liste lässt sich auch in ein übersichtliches Excel-Tabellenformat übertragen, einfach die erzeugte *.txt-Datei mit Excel öffnen. Auch nach einer Basisinstallation kann man sich eine Übersichtsliste der Standarddiensteinstellungen ablegen.
2. Bevor ein Dienst angehalten oder deaktiviert wird, sehen wir uns die Eigenschaften des jeweiligen Dienstes genauestens an, informieren uns über dessen Funktion - unter Berücksichtigung des installierten Soft- u. Hardwareequipments - und vor allem: wir kontrollieren die Abhängigkeiten des Dienstes, um Fehlfunktionen zu vermeiden!
3. Diensteinstellungen wirken sich global auf das gesamte Betriebssystem aus, und sind für jeden Benutzer am System gültig.
4. Bei Unsicherheiten betreffend einer Diensteinstellung, gilt die Empfehlung diesen auf „manuell" zu setzen. Der manuelle Status erlaubt dem Betriebssystem den Dienst bei Anforderung eines Programme oder einer Anwendung selbst zu starten.
5. Sollten sich einige Dienste in unserer nachstehenden Auflistung nicht auf eurem System befinden, dann kann dies eventuell vom Hersteller und dessen Vorinstallation abhängig sein und trifft in den meisten Fällen auf die Installation einer OEM Version der Windows XP Home-Edition zu.
6. Unsere Angaben beziehen sich auf die Version von Windows XP Professional inkl. Servicepack 2 (SP 2) und auf Windows 2000 inkl. Servicepack 4. Für Abweichungen von XP SP 1 zu XP SP 2 wurde ein Vermerk hinzugefügt.

- Ablagemappe
  Die Ablagemappe ist eine Erweiterung der Zwischenablage, die darin enthaltenen Informationen können anderen Benutzern im Netzwerk verfügbar gemacht werden und über Remotecomputer ausgetauscht werden.
  Standard: manuell
  Empfehlung: deaktivieren (nicht in Netzwerkumgebungen!)
  System: Windows 2000/XP

- Anmeldedienst
  Unterstützt die Durchsatzauthentifizierung von Kontoanmeldungsereignissen für Computer in einer Domäne und wird für den Aufbau einer sicheren Verbindung zu einem Domänencontroller verwendet.
  Standard: manuell
  Empfehlung: deaktivieren (nicht in Netzwerkumgebungen!)
  System: Windows 2000/XP

- Anwendungsverwaltung
  Stellt Softwareinstallationsdienste für Anwendungen, die über Systemsteuerung/Software installiert wurden, bereit. Dieser Dienst verarbeitet Anfragen zur Auflistung, Installation und auch zur korrekten Deinstallation von Software.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Die Windows Installations- u. Deinstallationsroutine funktioniert nicht mehr.

- Arbeitsstationsdienst
  Dieser Dienst erstellt und wartet Clientnetzwerkverbindungen mit Remoteservern.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Es gibt keine Verbindung zu anderen Rechnern innerhalb eines Windows-Netzwerkes.

- ASP.net
  Dieser Diensteintrag erscheint, wenn NetFramework installiert wird und das System komplett gepacht wurde. ASP.net sollte bei der Verwendung von entsprechenden Programmen, wie z.B. den aktuellen ATI Grafikkartentreiber auf manuell betrieben werden.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP

- Automatische Updates
  Stellt die Funktion zum automatischen Download und der Installation von Windows-Updates, wie Servicepacks, Patches und Hotfixes zur Verfügung. Von einer Deaktivierung ist dringend abzuraten, da anschließend kein Download mehr möglich ist!
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP

- COM+-Ereignissystem
  Unterstützt die automatische Verteilung von Ereignissen an COM-Komponenten, wie beispielsweise den Systemereignis-Benachrichtigungsdienst (System Event Notification Service).
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Der Nachrichtendienst für Systemereignisse arbeitet nicht mehr.

- COM+ Systemanwendung
  Verwaltet die Komponentenkonfiguration und -Überwachung von COM+-basierten Komponenten. COM+ stellt transparente Dienste zur Verfügung, beispielsweise Transaktionen, Sicherheit, Lastverteilung und Ressourcenmanagement innerhalb des Betriebssystems.
  Standard: manuell
  Empfehlung: manuell (nicht in Netzwerkumgebungen)

System: Windows XP
Konsequenz bei deaktiviertem Dienst: Mehrere Systemkomponenten funktionieren nicht mehr.

- Computerbrowser
  Führt eine aktuelle Liste der vorhandenen Computer im Netzwerk und gibt diese an „suchende" Computer und Anwendungen weiter. Kurzum, der Computerbrowser verwaltet die Liste aller Computer in einer Netzwerkumgebung. Bei einem Einzelplatzrechner kann man diesen Dienst deaktivieren.
  Standard: automatisch
  Empfehlung: deaktivieren (in Netzwerkumgebungen sollte der Dienst auf automatisch gestellt werden!)
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Keine Kommunikation in einem vorhandenen Netzwerk.

- DCOM-Server-Prozessstart **
  Bietet Startfunktionalität für diverse DCOM-Dienste nach der Installation des SP 2.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows XP
  Konsequenz bei deaktiviertem Dienst: Bei Deaktivierung gibt es Probleme mit dem RPC-Server in Form von Fehlermeldungen wie z.B. "Der RPC-Server ist nicht verfügbar"...

- Designs
  Dieser Dienst stellt die Designverwaltung von Benutzerdesigns zur Verfügung. Dabei handelt es sich z.B. um vordefinierte Symbole, Farben, Schriftarten und Fensterelementen. Auch der Wechsel zwischen klassischem oder XP-Design wird von diesem Dienst verwaltet.
  Standard: automatisch
  Empfehlung: deaktiviert
  System: Windows XP
  Konsequenz bei deaktiviertem Dienst: Die Anzeige der Schaltflächen, Fenster, und weiterer Steuerelementen wie Bildlaufleisten, werden nur mehr im Design "Windows-klassisch" angezeigt. Durch das klassische Design gewinnen ältere PC-Systeme aber auch klar an Performance.

- DHCP-Client
  Verwaltet die Netzwerkkonfiguration eines Computers, indem IP-Adressen und DNS-Namen automatisch registriert und aktualisiert werden.
  Standard: automatisch
  Empfehlung: manuell (nur bei Einzelplatzrechnern!. Wenn dynamische IP-Adressen verwendet werden, z.B. durch Zuweisung eines Internet Providers, muss dieser Dienst auf "automatisch" gesetzt werden, da ansonsten keine dynamischen IP-Adressen mehr empfangen werden können.
  System: Windows 2000/XP

- Dienst für Seriennummern der tragbaren Medien **
  Durch diesen Systemdienst werden die Seriennummern aller am Computer angeschlossenen tragbaren Audioplayer abgerufen. Dadurch können Medieninhalte auf sichere Weise auf diese Geräte kopiert werden. Ohne die entsprechende Seriennummer können die Inhalte dem jeweiligen Gerät nicht zugeordnet werden und die Übertragung von geschützten Inhalten kann verweigert werden. Der WMDM PMSP Dienst wird zusammen mit dem Windows Media Player 7 unter Windows 2000 installiert. Der Service kann in der Verwaltung deaktiviert werden, wenn man den Media Player nicht nutzt. Ab SP 2 wurde dieser Dienst im Standard von „automatisch" auf „manuell" gesetzt.
  Standard: manuell
  Empfehlung: deaktiviert
  System: Windows XP

- "Ausführen als"
  Das Starten von Prozessen unter alternativen Anmeldeinformationen, wird durch diesen Dienst

ermöglicht, wenn dies z.B. von diversen Programmen gefordert wird. In Windows 2000 ist dieser Dienst auch unter "RunAs" bekannt. Programme können damit unter einem anderen Benutzer, als den aktuell angemeldeten Benutzer ausgeführt werden. Dieser Dienst wird primär von Administratoren verwendet, die sich mit einem eingeschränktem Benutzerkonto anmelden und mithilfe dieser sekundären Anmeldung Anwendungen oder Programme temporär
als Administrator ausführen.
Standard: automatisch
Empfehlung: manuell
System: Windows 2000

- Distributed Transaction Coordinator
  Dieser Dienst steht als Transaktionsmanager zur Verfügung und dient z.B. der Koordination von zwei Datenbanken, Nachrichtenwarteschlangen (Message Queues), die über mehrere Computersysteme verteilt werden.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Der Datenaustausch zwischen diversen Ressourcenverwaltungen würde nicht mehr funktionieren.

- DNS-Client
  Der wichtige Systemdienst DNS-Client (Domain Name Service) löst DNS-Namen für den Computer auf und speichert diese zwischen.
  Standard: automatisch
  Empfehlung: manuell (nur bei Einzelplatzrechnern! Siehe auch DHCP-Client.)
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Zwischengespeicherte Domain-Namen würden nicht mehr verfügbar sein. Wenn dieser Dienst angehalten oder deaktiviert wird, kann der Computer in einem Netzwerk auch keine DNS-Namen mehr auflösen und in einer vorhandenen Domäne keine Active Directory-Domänencontroller finden!

- Druckwarteschlange
  Die Druckwarteschlange verwaltet alle lokalen und Netzwerkdruckwarteschlangen und lädt zudem die Dateien in den Arbeitsspeicher. Der so genannte Druckerspooler steuert alle Druckaufträge.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Das Verwalten von Druckaufträgen funktioniert nicht mehr und vom lokalen Drucker aus kann weder gedruckt, noch gefaxt werden. Achtung: wenn dieser Dienst einmal angehalten wurde, wird er nicht mehr automatisch gestartet, dies müsste händisch nachgeholt werden.

- Eingabegerätezugang
  Dieser Dienst ermöglicht einen Standardeingabezugang für spezielle Eingabegeräte, wie z.B. Maus, Tastatur, Joystick. Auch die Verwendung von vordefinierten Schnelltasten auf Tastaturen, Steuerungen von Hifi-Anlagen, DVD-Rekordern und Bluetooth-Anwendungen wird über diesen Dienst gewährleistet. Diese HID-Geräte (Human Interface Device) interagieren direkt mit dem Benutzer über die USB-Schnittstelle.
  Standard: deaktiviert
  Empfehlung: deaktiviert (sofern keine Geräte vorhanden sind, die diesen Dienst erfordern)
  System: Windows XP

- Ereignisprotokoll
  Das Ereignisprotokoll ermöglicht nicht nur die Anzeige der von Windows-Programmen und Komponenten ausgegebenen Protokoll- und Fehlermeldungen, sondern dient uns vor allem zur Analyse und Nachverfolgung diverser System- und Anwendungsfehler, wie auch der System- und Zugriffsüberwachung. Damit erhalten wir sehr wichtige Diagnoseinformationen.

Dieser Dienst kann somit aus gutem Grunde nicht angehalten werden. Eine Deaktivierung sollte keinesfalls erfolgen!
Standard: automatisch
Empfehlung: automatisch
System: Windows 2000/XP

- Faxdienst
  Der Faxdienst stellt uns unter Windows 2000 die Faxfunktion für den Computer bereit. Dies erfolgt entweder über ein lokales Faxgerät oder ein freigegebenes Netzwerk-Faxgerät. Häufig treten hier Fehler, respektive eine Nichtfunktion auf, wenn die Dienste Druckwarteschlange oder Telefonie deaktiviert wurden, von denen der Faxdienst abhängig ist.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000

- Fehlerberichterstattungsdienst
  Der Fehlerberichterstattungsdienst erkennt und speichert unerwartete Anwendungsbeendigungen und meldet diese auf vorheriger Anfrage an den Benutzer per Dialogfenster an Microsoft. Im administrativen- und Supportbereich mag dies sinnvoll erscheinen, für den Heimbereich kann man diesen Dienst durchaus deaktivieren.
  Standard: automatisch
  Empfehlung: deaktiviert
  System: Windows XP

- Gatewaydienst auf Anwendungsebene
  Dieser sehr wichtige Dienst ist eine Unterkomponente des Dienstes "Internetverbindungsfirewall/Gemeinsame Nutzung der Internetverbindung" und ermöglicht für Protokoll-Plug-Ins von Drittanbietern die gemeinsame Nutzung der Internetverbindung und der Internetverbindungsfirewall.
  Standard: manuell
  Empfehlung: manuell
  System: Windows XP
  Konsequenz bei deaktiviertem Dienst: Diverse Programme können keine Verbindung in das Internet herstellen, wie z.B. das Senden von Nachrichten über den Windows Messenger oder ähnliche Programme, um nur ein Beispiel zu nennen.

- Gemeinsame Nutzung der Internetverbindung
  Dieser Windows 2000 spezifische Dienst bietet allen Rechnern über eine vorhandene DFÜ-Verbindung Netzwerkadressübersetzungs- und Namensauflösungsdienste an, vorwiegend sinnvoll in einem Heimnetzwerk.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000

- Geschützter Speicher
  Ein immens wichtiger Prozess im Dienste der gesamten Systemsicherheit! Durch diesen Dienst werden wichtige Informationen, wie etwa der private Schlüssel oder Kennwörter, die sich im verwendeten Speicher befinden, geschützt und der Zugriff durch nicht autorisierte Benutzer, Dienste und Prozesse wird dadurch verhindert. Der bereitgestellte Speicherort ist somit vor unzulässigen Änderungen sicher.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Der Speicherinhalt ist nicht mehr geschützt, und private Schlüssel sind nicht mehr zugängig. Grund genug, diesen Dienst niemals anzuhalten oder gar zu deaktivieren!

- Hilfe und Support
  Dieser Dienst aktiviert das Hilfe- und Supportcenter auf eurem Computer. Da das Hilfe und

Supportcenter eine ganze Reihe sehr informativer Unterstützung bereitstellt, sollte ihr diesen Dienst nicht deaktivieren, es sei denn ihr wißt schon alles...
Standard: Automatisch
Empfehlung: manuell
System: Windows 2000/XP

- Hilfsprogramm-Manager
  Dieser Dienst startet und konfiguriert Hilfsprogramme wie die Bildschirmlupe und die Bildschirmtastatur.
  Standard: manuell
  Empfehlung: deaktiviert
  System: Windows 2000

- IMAPI-CD-Brenn-COM-Dienste
  Das Brennen von CDs über Windows, respektive die IMAPI-COM-Schnittstelle wird durch diesen Dienst unterstützt und verwaltet.
  Standard: manuell
  Empfehlung: deaktiviert sofern Brennprogramme von Drittherstellern verwendet werden.
  System: Windows XP

- Indexdienst
  Der Indexdienst indiziert Inhalt und Eigenschaften von Dateien auf lokalen Computern und Remotecomputern und ermöglicht über eine flexible Abfragesprache den schnellen Zugriff auf die Dateien. Auch für die schnelle Dokumentsuche auf lokalen Computern wird dieser Dienst verwendet. Fakt ist aber auch, dass dieser Dienst einen mächtigen Anteil an Ressourcen vom Arbeitsspeicher und der CPU abverlangt. An sich sollte der Indexdienst nur im Leerlaufzustand des Systems ausgeführt werden, Erfahrungen haben aber gezeigt, dass sich dieser Dienst auch außerhalb dieser Zeiten aktiv bewegt. Das ist unakzeptabel und macht keinen Sinn.
  Standard: manuell
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- Infrarotüberwachung
  Dieser Dienst nterstützt auf dem Computer installierte Infrarotgeräte, sucht nach anderen Geräten in Reichweite und baut entsprechende Verbindungen auf. Wer keine Infrarotgeräte verwendet, kann den Dienst getrost deaktivieren, es gibt keine problematischen Abhängigkeiten.
  Standard: Automatisch
  Empfehlung: deaktiviert
  System: Windows XP

- Intelligenter Hintergrundübertragungsdienst
  Bietet einen Dateiübertragungsmechanismus und Warteschlangenmanager an, der im Hintergrund ausgeführt wird um Dateien asynchron zwischen Client und HTTP-Server zu übertragen. Klassisches Beispiel dafür ist das Windows-Update über die Microsoft Website. Genutzt wird diese Übertragung, wenn anderweitig keine Netzwerkkapazitäten verwendet werden. Wenn eine Verbindung unterbrochen wird oder der Benutzer sich abmeldet, bleibt die Verbindung dieses Dienstes bestehen, sobald sich der Benutzer neu anmeldet, wird der Übertragungsvorgang wieder aufgenommen.
  Standard: manuell
  Empfehlung: manuell
  System: Windows XP
  Konsequenz bei deaktiviertem Dienst: Es werden keine automatischen Updates mehr heruntergeladen. Entscheidend ist dieser Faktor vor allem beim Einsatz des Softwareaktualisierungsdienst (SUS), wenn dieser Dienst über eine Gruppenrichtlinie konfiguriert wurde!

- IPSec-Richtlinien-Agent (IPSec-Dienst) **
  Die End-to-End-Sicherheit zwischen Clients und Servern wird mit diesem Dienst ermöglicht.

Damit auch eine Paketfilterung und Aushandlung zwischen sendenden und empfangenden Computern in IP-Netzwerken. IPSec bietet zudem Sicherheit für VPN-Verbindungen, die das Layer-Two-Tunneling-Protokoll (L2TP) verwenden.
Standard: automatisch
Empfehlung: automatisch
System: Windows 2000/XP
Konsequenz bei deaktiviertem Dienst: Wenn dieser Dienst angehalten wird, ist die TCP/IP-Sicherheit zwischen Clients und Servern im Netzwerk nicht mehr gegeben.

- Kompatibilität für schnelle Benutzerumschaltung
  Für ein Mehrfachbenutzersystem wird dieser Dienst benötigt, um die schnelle Benutzerumschaltung anzubieten, ohne dass der angemeldete Benutzer seine laufenden Programme beenden muss. Befindet sich auf dem System jedoch nur ein aktives Benutzerkonto, kann man diesen Dienst deaktivieren.
  Standard: manuell
  Empfehlung: manuell
  System: Windows XP

- Konfigurationsfreie drahtlose Verbindung
  Benötigt man für die automatische Konfiguration für 802.11-Adapter und kabellose Netzwerkgeräte.
  Standard: automatisch
  Empfehlung: deaktiviert (wenn keine drahtlosen Übertragungsgeräte wie z.B. W-LAN vorhanden sind. PDA's, die sich mit dem Computer über „hot sync" abgleichen, erfordern diesen Dienst)
  System: Windows XP

- Kryptografiedienste
  Als Hauptaufgabe bestätigt dieser Dienst die Echtheit der Signaturen von Windows Dateien. Auch das manuelle und automatische Windows-Update erfordert diesen Dienst.
  Sehen wir uns aber die Unterteilung genauer an. Dies besteht aus drei Verwaltungsdiensten:

  1. Katalogdatenbankdienst, der für das Hinzufügen, Entfernen und Durchsuchen von Katalogdateien verantwortlich ist. Diese werden verwendet, um die Dateien im Betriebssystem zu signieren. Die Treibersignatur und der Windows Dateischutz sind z.B. auf diesen Dienst angewiesen.
  2. Dienst für geschützten Stammspeicher, der für das Hinzufügen und Entfernen von Zertifikaten vertrauenswürdiger Stammzertifizierungsstellen verantwortlich ist.
  3. Der Schlüsseldienst ermöglicht es Administratoren Zertifikate im Auftrag des lokalen Computerkontos zu registrieren.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows XP

- Leistungsprotokolle und Warnungen
  Dient zur Erfassung von zeitgeplanten Systemleistungsdaten, von lokalen Computern oder Remotecomputern. Der Systemmonitor sei hier als Beispiel genannt. Dieser Dienst wird nur ausgeführt, wenn mindestens eine Sammlung aktiv geplant wurde. Als sinnvoll erachten wir diesen Dienst nur in einer Serverumgebung.
  Standard: manuell
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- MS Software Shadow Copy Provider
  Dieser Dienst verwaltet softwarebasierte Schattenkopien, die durch den weiteren Dienst Volumeschattenkopie erstellt wurden. Mit einer Schattenkopie wird eine „Snapshotkopie" eines Datenträgers respektive einer Partition erstellt. Dieser zu einem bestimmten Zeitpunkt erstellte Snapshot bleibt unverändert bestehen, so dass mit einer Anwendung, wie beispielsweise dem Windows-Backup-Programm Daten gesichert werden. Dies gilt auch für

den Einsatz von Sicherungssoftware von Drittherstellern, wie z.B. Norton Ghost vom Hersteller Symantec oder ein vergleichbares Imageprogramm.
Standard: manuell
Empfehlung: manuell
System: Windows XP
Konsequenz bei deaktiviertem Dienst: Backup/Imageprogramme funktionieren nicht mehr.

- Nachrichtendienst **
  Mittels des Befehls NET SEND werden zwischen Client und Server in einer Netzwerkumgebung Warnmeldungen ausgetauscht. In einer Einzelplatzumgebung benötigen wir diesen Service nicht, zudem deaktivieren diesen auch aus Gründen der Sicherheit. Erst ab SP 2 wurde dieser Dienst von Microsoft von der Standardeinstellung „automatisch" auf „deaktiviert" gestellt und wir haben nicht vor, daran etwas zu ändern. Achtung: wenn ihr Windows 2000 oder XP inkl. SP 1a verwendet, dann sollte der Dienst auf „deaktiviert" gestellt werden! Der Nachrichtendienst hat nichts mit dem MSN-Messenger zu tun.
  Standard: deaktiviert
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- NetMeeting-Remotedesktop-Freigabe
  So genannte Netzwerkkonferenzen werden damit ermöglicht. Dies gilt natürlich nur für autorisierte Benutzer, die z.B. von einem anderen Computer aus über das firmeneigene Intranet mit der Software NetMeeting auf ihren Windows-Desktop zugreifen. Diese Freigabe ist aber auch ein offenes Tor für ungebetene Gäste.
  Standard: manuell
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- Netzwerk-DDE-Dienst **
  DDE steht für „Dynamic Data Exchange", also den dynamischen Datenaustausch und dient dem sicheren Netzwerktransport. DDE kann z.B. über Netzwerkfreigaben stattfinden, indem die zwischengespeicherten Daten mit einem anderen Computer im Netzwerk ausgetauscht werden. In einer Einzelplatzumgebung macht dieser Dienst wenig Sinn, da die lokale Zwischenablage davon nicht betroffen ist. Ab SP 2 wurde dieser Dienst von „manuell" auf „deaktiviert" gesetzt. Wir behalten diese Einstellung bei.
  Standard: deaktiviert
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- Netzwerk-DDE-Serverdienst **
  Ähnlich dem DDE-Dienst verwaltet der Serverdienst Netzwerkfreigaben, über die DDE-Übertragungen laufen.
  Standard: deaktiviert
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- Netzwerkverbindungen
  Dieser Dienst verwaltet Objekte im Ordner Netzwerkverbindungen, und ist für die Netzwerkkonfiguration auf dem Rechner verantwortlich. Dies gilt für LAN (Local Aera Network), wie auch für WAN (Wide Area Netzwork) Umgebungen. An sich wird dieser Dienst automatisch gestartet, wenn der Starttyp auf „manuell" eingestellt ist und die Netzwerkverbindungsschnittstelle angefordert wird. Sollte ein Internetverbindungsaufbau trotz manueller Einstellung nicht erfolgen, dann ist die Einstellung auf „automatisch" zu setzen.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Bereits erstellte Verbindungen im Ordner „Netzwerkverbindungen" werden nicht mehr angezeigt. LAN-Einstellungen können nicht

konfiguriert werden, eine eventuell gemeinsame Nutzung einer Internetverbindung funktioniert nicht ordnungsgemäß, es können keine neuen Verbindungen erstellt werden.

- Netzwerkversorgungsdienst **
  Dieser Dienst verwaltet XML-Konfigurationsdateien auf Domänenbasis für die automatische Netzwerkversorgung. Der Service ist nach der Installation von SP 2 verfügbar.
  Standard: manuell
  Empfehlung: manuell
  System: Windows XP

- NLA (Network Location Awareness)
  NLA erfasst und speichert Netzwerkkonfigurationsinformationen, wie z.B. IP-Adressen, Domänennamenänderungen sowie Informationen über Speicherortänderungen, und benachrichtigt bei Änderung Anwendungen. Ab SP 2 wird dieser Dienst nicht mehr benötigt.
  Standard: manuell
  Empfehlung: deaktiviert
  System: Windows XP

- NT-LM-Sicherheitsdienst
  Bietet Sicherheit für Remoteprozeduraufrufe (RPC), die andere Transportwege als Named Pipes (Pufferspeicher, die zur Kommunikation zwischen zwei Prozessen benutzt werden) verwenden. Die Serveranwendung Telnet würde z.B. diesen Dienst benötigen.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Serverbasierende Programme starten nicht mehr.

- Plug & Play
  Dieser Dienst stellt das Zentrum der automatischen Hardwareerkennung dar. Die Hardwareänderung auf einem System wird damit in den meisten Fällen ohne Benutzereingabe erkannt werden. Eine manuelle Konfiguration muss nur selten vorgenommen werden. Einfachstes Beispiel zeigt den Anschluss einer USB-Tastatur oder Maus an, die durch Plug & Play sofort als neues Gerät erkannt wird. Windows sucht automatisch nach dem geeigneten Treiber für das Gerät. Dieser sehr wichtige Dienst darf nicht angehalten oder deaktiviert werden.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Die Erkennung von Plug & Play Geräten funktioniert nicht mehr und Im Gerätemanager werden keine Hardwaregeräte mehr angezeigt.

- QoS-RSVP
  QoS (Quality of Service) unterstützt nicht nur die Bandbreitenkontrolle in einem Netzwerk, durch das Ressource Reservation Protokoll(RSVP) wird auch die Reservierung von Bandbreiten in IP-basierten Netzen ermöglicht. RSVP ist notwendig, um diese Dienste-Qualitäten zu realisieren. Beispielsweise um Datenströmen, insbesondere bei Audio- und Video-Übertragungen mittels Internet , durch Bandbreiten-Reservierung eine gute Qualität zu garantieren. Dieser Service wird benötigt, wenn wir z.B. den Windows-Media-Player oder NetMeeting verwenden. Dafür genügt aber die Einstellung „manuell". Bei Nichtverwendung dieser Programme kann der Dienst deaktiviert werden.
  Standard: automatisch
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- RAS-Verbindungsverwaltung
  Dieser Dienst stellt eine Netzwerkverbindung her und verwaltet DFÜ- und VPN-Verbindungen zwischen unserem Computer und dem Internet oder anderen Remotenetzwerken. Von daher ist dieser Dienst auch stets betriebsbereit, für den Fall, dass eine Netzwerkverbindung aufgebaut werden soll.

Standard: manuell
Empfehlung: manuell
System: Windows 2000/XP
Konsequenz bei deaktiviertem Dienst: Es kann keine Netzwerkverbindung, wie z.B. eine Internetverbindung aufgebaut werden. Im Zweifelsfalle oder bei Verbindungsproblemen, kann dieser Dienst auf „automatisch“ gesetzt werden.

- Remoteprozeduraufruf (RPC)
  Mit diesem Dienst sind wir bei einem sehr maßgeblichen Punkt für die volle Funktion unseres Betriebssystems angelangt. Eine Vielzahl von anderen Diensten ist davon abhängig, dass RPC gestartet ist! Dies wird uns auch rasch verdeutlicht, wenn wir versuchen den Dienst zu deaktivieren, denn dies wird uns unter Windows XP erst gar nicht ermöglicht. Unter Windows 2000 bleibt diese Option offen, jedoch wäre das Betriebssystem bei Deaktivierung von RPC nicht mehr bootfähig.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP
  Konsequenz bei deaktiviertem Dienst: Betriebssystem kann nicht mehr gestartet werden!

- Remote-Registrierung
  Unter Windows 2000 bekannt als „Remote-Registrierungsdienst“ und ist verantwortlich für das Ändern von Registrierungseinstellungen auf einem Domänencontroller, unter Voraussetzung, dass die Remotebenutzer über die erforderlichen Berechtigungen verfügen. Im Standard sind das nur Administratoren und Benutzer der Gruppe der Sicherungs-Operatoren, die auf die Registrrierung Zugriffrechte haben. Zudem wird dieser Dienst für die Anwendung des Microsoft Baseline Security Analyzer (MBSA) benötigt. Damit kann der aktuelle Sicherheitsstand in Sachen Patches und Updates auf dem System überprüft werden. Sollte MBSA nicht eingesetzt werden, können wir diesen Dienst deaktivieren.
  Standard: automatisch
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- Routing und RAS **
  Bietet das Einwählen über einen lokalen Computer durch ein Modem oder andere Verbindungsgeräte an, der Fernzugriff auf ein lokales Netzwerk benötigt. Dieses Multiprotokoll bezieht sich auf –LAN -> LAN, LAN -> WAN, sowie auf VPN- und NAT-Routingdienste. Wenn kein Bedarf an diesen Fernverbindungen besteht, ist dieser Dienst unnötig. Mit SP 2 wurde die Standardeinstellung von „manuell“ auf „deaktiviert“ gesetzt.
  Standard: deaktiviert
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- RPC-Locator
  Dieser Systemdienst ermöglicht RPC-Clients, die Suche nach RPC-Servern. Auch die RPC-Namensdienstdatenbank wird damit verwaltet. Dieser Dienst wird nur mehr in seltenen Fällen in einem Netzwerk benötigt, und wäre im Bedarfsfall auf „automatisch“ zu setzen.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP

- Sekundäre Anmeldung
  Die sekundäre Anmeldung ist mit dem Dienst "Ausführen als" unter Windows 2000 gleichzusetzen. Lediglich der Dienstname lautet hier anders, die Funktion ist dieselbe.
  Standard: automatisch
  Empfehlung: manuell
  System: Windows XP

- Server
  Die gemeinsame Nutzung von lokalen Ressourcen wie Datenträgern und Druckern wird mit

dem Serverdienst ermöglicht, damit andere Benutzer im Netzwerk darauf zugreifen können. Aus Sicherheitsgründen sollte dieser Dienst deaktiviert werden, sofern kein Zugriff auf die genannten Objekte innerhalb eines Netzwerkes erfolgen muss.
Standard: automatisch
Empfehlung: deaktiviert
System: Windows 2000/XP

- Shellhardwareerkennung
  Dient zur Überwachung von AutoPlay-Geräten, wie z.B. Memory Cards und CD-Player. Aber auch für den korrekten Autostart von eingelegten CD/DVD Medien ist dieser Dienst verantwortlich. AutoPlay unterstützt unterschiedlichste Medientypen und Anwendungen, wie z.B. Wechselspeichermedien, Flash Medien und auch externe Hot-Plug-USB-Festplatten. Da in der Praxis sehr häufig mit diesen Medien gearbeitet wird, sollte dieser Dienst automatisch gestartet werden.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows XP

- Sicherheitscenter **
  Dieser Dienst wurde mit SP 2 unter Windows XP eingeführt und zeichnet den Status der Automatischen Updates, der Windows-Firewall und installierter Antivirus-Software auf. Wenn Updates manuell gestartet werden, und eine Firewall von einem Drittthersteller verwendet wird, kann man auf dieses Sicherheitscenter getrost verzichten. Neuesten Meldungen zufolge stellt das Sicherheitscenter unter SP 2 aber auch ein Risiko dar. Die Statusdaten könnten von potentiellen Angreifern von außen eingesehen werden, im schlimmsten Fall sind diese in der Lage dem Benutzer falsche Statusinformationen unterzuschieben. Eine Deaktivierung dieses Dienstes genügt aber nicht, denn nach einem Neustart, wird dieser Dienst wieder auf „automatisch“ gesetzt und somit gestartet. Im gestarteten Dienstmodus nehmen wir nun folgende Schritte vor:

  Über Start -> Systemsteuerung gelangen wir in das Sicherheitscenter und klicken auf der linken Seite des Fensters auf den Link „Warneinstellungen des Sicherheitscenters ändern“. Die drei Checkboxen für Firewall, Automatisches Update und Antivirenschutz haken wir aus. Nun setzen wir den Dienst wieder auf „deaktiviert“, und nach einem Neustart bleibt uns dieser Status nun auch erhalten.
  Standard: automatisch
  Empfehlung: deaktiviert
  System: Windows XP

- Sicherheitskontenverwaltung
  Dieser sehr wichtige Dienst verwaltet alle Benutzer- und Gruppenkonten auf dem System. Diese Sicherheitskonten werden in der SAM (Security Account Manager) über die Registrierung gespeichert. Dies gilt ausschließlich für den lokalen Computer. Auf einem Domänencontroller werden die Sicherheitskonten in der Active Directory gespeichert. Dieser Dienst kann nicht angehalten werden und darf keinesfalls deaktiviert werden!
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP

- Sitzungs-Manager für Remotedesktophilfe
  Dient zur Verwaltung und Assistenz der Remotehilfe über das Hilfe-u. Supportcenter unterstützt.
  Standard: manuell
  Empfehlung: deaktiviert
  System: Windows XP

- Smartcard
  Verwaltet und steuert den Zugriff auf angeschlossene Smartcard-Lesegeräte mit eingelegter Smartcard. Eine Smartcard ist eine Chipkarte mit integriertem Microprozessor und Speicher,

die in unterschiedlichster Anwendung zum Einsatz kommt, wie z.B. Speicherkarten oder digitales Fernsehen.
Standard: manuell
Empfehlung: deaktiviert
System: Windows 2000/XP

- Smartcard-Hilfsprogramm **
  Dieser Dienst wird nach der Installation von SP 2 unter Windows XP entfernt und mit dem Dienst „Smartcard" kombiniert.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP

- SSDP-Suchdienst
  Dieser Dienst sucht nach angeschlossenen UPnP-Geräten (Universal Plug & Play). Achtung: UpnP ist nicht mit PnP (Plug & Play) gleichzusetzen! UpnP-Geräte können z.B. Alarmanlagen, Überwachungskameras, und diverse Multimediageräte sein, die über den PC vernetzt gesteuert werden. Fakt ist, dass dieser Dienst permanent im Hintergrund läuft und nach Geräten dieser Art sucht. Dadurch verursacht dieser Service eine nicht geringe CPU-Auslastung. Mitunter dürfen wir hierbei auch das Sicherheitsrisiko nicht außer Acht lassen. Microsoft hatte dafür den UpnP-Patch bereitgestellt, damit ein Überlauf des Speicherpuffers, der ein Eindringen von ungebetenen Gästen ermöglicht, verhindert wird. Manche Multiplayer-Games benötigen für den Verbindungsaufbau diesen Dienst auf „automatisch". Achtet darauf, dass ihr über alle aktuellen Sicherheitsupdates verfügt, wenn dieser Dienst läuft.
  Standard: manuell
  Empfehlung: deaktiviert
  System: Windows XP

- Systemereignisbenachrichtigung
  Dieser Dienst ist Teil des Svchost Systems, überwacht und verfolgt Systemereignisse wie etwa Windows-Netzwerkanmeldungen, Stromversorgungsereignisse und steht in direkter Verbindung zum COM+ Ereignissystem.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP

- Systemwiederherstellungsdienst
  Ein Service unter Windows XP, über den sich die Geister scheiden. Dieser hat zwar den Vorteil, ein nicht mehr funktionierendes System in einen vorherigen funktionierenden Zustand wiederherzustellen. Der Dienst erstellt für jede neue Installation eines Programms oder eines Treibers einen sogenannten Wiederherstellungspunkt. Da der Dienst bei Aktivierung permanent im Hintergrund läuft, belastet er nicht nur die Systemperfomance um ein Wesentliches, es bedarf für diesen Service auch eine Menge an Speicherplatz auf der Festplatte und dieser kann sich durchaus im Gigabytebereich bewegen. Bei einer großen Festplatte kann man mit 10-20 Gigabyte Speicherplatz für die Wiederherstellungspunkte durchaus rechnen. Für die Stabilität unseres Betriebssystems gewinnen wir durch die Systemwiederherstellung nichts. Weit effektiver und sicherer ist nach wie vor ein sauberes Image zur Systemwiederherstellung im Notfall.
  Standard: automatisch
  Empfehlung: deaktiviert
  System: Windows XP

- Taskplaner
  Durch den Taskplanerdienst können unterschiedliche geplante, zeitgesteuerte Aufgaben vom System durchgeführt werden, wie z.B. Wartungsarbeiten oder automatisierte Backup-Szenarien. Antivirenprogramme von Drittherstellern benötigen diesen Dienst für ein automatisches Update ebenso, wie alle System-u. Patchupdates.
  Standard: automatisch

Empfehlung: automatisch
System: Windows 2000/XP

- TCP/IP-NetBIOS-Hilfsprogramm
  Die Unterstützung von NetBIOS-und-TCP/IP-Diensten, sowie die NetBIOS-Namensauflösung wird durch diesen Service geboten. Dadurch wird Benutzern die Freigabe von Dateien und Druckern sowie die Anmeldung im Netzwerk ermöglicht. Wenn kein Netzwerk vorhanden ist, und auch das WINS-Protokoll nicht verwendet werden muss, ist dieser Dienst für einen Einzelplatzrechner nicht nötig.
  Standard: automatisch
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- Telefonie
  Dieser Dienst kontolliert Telefonie-Geräte auf dem lokalen Computer und wird zwingend für Dial-up Modems respektive Verbindungen benötigt. Telefonie steht auch in direkter Verbindung mit RAS-Anwendungen.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP

- Telnet
  Ermöglicht Terminalsitzungen für Telnet-Clients in einer Netzwerkumgebung. Darüber kann sich ein Benutzer remote an einem Server anmelden. Der Dienst stellt ein beträchtliches Sicherheitsrisiko dar und wird auf einem Einzelplatzrechner für den Heimbetrieb nicht benötigt.
  Standard: manuell
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- Terminaldienste
  Auch dieser Dienst erlaubt einen Fernzugriff auf einen lokalen Computer. Terminaldienste bieten damit eine Multisessionumgebung an, die Clientgeräten den Zugriff auf eine virtuelle Windows-Desktopsitzung ermöglicht. Der schnelle Benutzerwechsel unter Windows XP erfordert diesen Dienst ebenfalls.
  Standard: manuell
  Empfehlung: manuell
  System: Windows XP

- Treibererweiterungen für Windows-Verwaltungsinstrumentation
  WMI (Windows Management Instrumentation) dient der Unterstützung von Systemverwaltungsinformationen von Treibern. und bietet einem Programmierer einen einheitlichen Weg um Daten über das lokale System oder komplette Netzwerk-Installationen einzuholen.
  Standard: manuell
  Empfehlung: manuell
  System: Windows XP

- Überwachung verteilter Verknüpfungen (Client)
  Verwaltet Verknüpfungen zwischen NTFS-Dateien in Computern oder zwischen Computern in einer Netzwerkdomäne. Wenn beispielsweise eine Datei auf Rechner A erzeugt wird, und für diese auf Rechner B ein Link oder Short Cut gesetzt wird, dann informiert dieser Dienst Rechner B, sobald auf Rechner A eine Pfadänderung vorgenommen wurde.
  Standard: automatisch
  Empfehlung: manuell
  System: Windows 2000/XP

- Universeller Plug & Play-Gerätehost**
  Dieser Dienst ist ab SP 2 verfügbar und steht in Verbindung mit dem SSDP-Suchdienst,

erkennt und konfiguriert UpnP-Geräte im Heimnetzwerk, wie z.B. SAT, TV, Video-Geräte oder gar die Mikrowelle, die sich über den PC steuern ließe. Wenn derartige Geräte nicht verwendet werden, sollte der Dienst aus Sicherheitsgründen unbedingt deaktiviert werden. Wird der Dienst aus Bedarfsgründen doch benötigt, dann ist es unumgänglich, dass euer System mit allen aktuellen Sicherheitspatches versehen ist.
Achtung: UPnP ist nicht zu verwechseln mit dem Plug & Play Dienst!
Standard: manuell
Empfehlung: deaktiviert
System: Windows XP

- Unterbrechungsfreie Stromversorgung
  Dieser Systemdienst verwaltet eine an den Computer angeschlossene unterbrechungsfreie Stromversorgung (USV). Sinnvoll ist dieser Service hauptsächlich im Server-Netzwerkbereich, um bei Stromausfall ein Weiterarbeiten zu gewährleisten.
  Standard: manuell
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- Upload-Manager **
  Dieser Dienst ist nach der Installation von SP 2 unter Windows XP nicht mehr vorhanden und war bis dahin für die Verwaltung von synchronen und asynchronen Dateiübertragungen zwischen Clients
  und Servern im Netzwerk verantwortlich.
  Standard: automatisch
  Empfehlung: deaktiviert (nur mehr gültig für Windows XP mit SP 1a)
  System: Windows XP

- Verwaltung für automatische RAS-Verbindung
  Erstellt eine Verbindung in einer Netzwerkumgebung, wenn diese von einer Remote-Adresse angefordert wird. Dieser Dienst kann für den Aufbau der Internetverbindung benötigt werden, dies hängt aber letztendlich vom Internet Provider und dessen Logon Prozessen ab.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP

- Verwaltung logischer Datenträger
  Dieser Dienst überwacht neue Festplattenlaufwerke und auch Plug & Play-Ereignisse für erkannte neue Laufwerke und übergibt diese Informationen an den Verwaltungsdienst für die Verwaltung logischer Datenträger weiter. Wenn dynamische Datenträger (z.B. auch für ein RAID) in einem System verwendet werden, ist dieser Dienst zwingend erforderlich.
  Standard: automatisch
  Empfehlung: manuell
  System: Windows 2000/XP

- Verwaltungsdienst für die Verwaltung logischer Datenträger
  Dient der Konfiguration von Festplattenlaufwerken und –Volumes, und wird nur gestartet, wenn ein Laufwerk oder eine Partition konfiguriert wird respektive, wenn ein neues Laufwerk erkannt wird. Danach wird der Dienst automatisch beendet.
  Standard: manuell
  Empfehlung: manuell (nur mehr gültig für Windows XP mit SP 1a)
  System: Windows 2000/XP

- Volumeschattenkopie
  Wird in Verbindung mit dem Dienst „MS Software Shadow Copy Provider" verwendet und verwaltet primär Datenträgersnapshots, die zur Sicherung dienen. Windows-Backup agiert direkt mit diesem Dienst.
  Standard: manuell
  Empfehlung: manuell
  System: Windows XP

- Warndienst **
  Der Warndienst benachrichtigt ausgewählte Benutzer und Computer über administrative Warnmeldungen, die mit dem Netzwerk verbunden sind. Auf einem Einzelplatzrechner wird dieser Dienst nicht benötigt. Ab SP 2 wurde die Standardeinstellung von „manuell" auf „deaktiviert" gestellt.
  Standard: deaktiviert
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- Webclient
  Dieser Dienst ermöglicht Win32-Anwendungen den Zugriff auf internetbasierende Dokumente. Einige Microsoft-Produkte wie der MSN-Messenger oder NetMeeting könnten nicht mehr funktionieren, wenn dieser Dienst deaktiviert ist. Dies war in unserem Testlauf mit MSN-Messenger jedoch nicht der Fall.
  Standard: automatisch
  Empfehlung: deaktiviert
  System: Windows XP

- Wechselmedien
  Verwaltet und katalogisiert austauschbare Medien, Geräte und Bibliotheken, einschließlich Datenbänder und CDs. In seltenen Fällen funktioniert AutoPlay bei Deaktivierung dieses Dienstes nicht mehr.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP

- Windows Audio
  Bietet Unterstützung für Sounds und Audiofunktionen. Dieser Dienst verwaltet zudem Plug & Play-Ereignisse für Audiogeräte, wie Soundkarten.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows XP

- Windows Installer
  Dieser sehr wichtige Dienst verwaltet die Installation und das Entfernen von Anwendungen und Programmen, die in Form von MSI-Installer Paketen aufliegen. Der Windows-Installer verwaltet zudem auch das Hinzufügen und Entfernen von Softwarekomponenten, überwacht den Dateizustand und bietet Notfallwiederherstellungen
  mithilfe von so genannten Rollbacks.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP

- Windows-Bilderfassung (WIA)
  WIA sorgt für die Bilderfassung für Scanner, Webcams und Kameras. In manchen Fällen erfordert dieser Dienst für USB-Geräte die automatische Startart.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP

- Windows Media Connect (WMC) **
  Bei einem Update auf den Mediaplayer 10 wird dieser Dienst installiert
  Windows Media Connect wird als Streaming-Serverdienst ab SP 2 angeboten. und erkennt z.B. über die USB-Schnittstelle angeschlossene oder Plug & Play angebundene Streaming-Clients und stellt auf Wunsch Medieninhalte wie Audio, Video, und Bilder zur Verfügung.
  Standard: manuell
  Empfehlung: manuell
  System: Windows 2000/XP

- Windows-Firewall/Gemeinsame Nutzung der Internetverbindung **
  Unter Windows 2000 wurde dieser Dienst als "Gemeinsame Nutzung der Internetverbindung" bezeichnet. Unter Windows XP SP 1a kennt man ihn unter dem Namen Internetverbindungsfirewall/Gemeinsame Nutzung der Internetverbindung. Dieser Systemdienst stellt über eine DFÜ- oder Breitbandverbindung, eine Netzwerkadressübersetzung (NAT), Adressierungs- und Namensauflösung, sowie auch Dienste zum Schutz vor Eindringversuchen im Heimnetzwerk oder kleinerem Firmennetzwerk bereit. Durch die Aktivierung dieses Dienstes wird der Rechner quasi zum "Server" respektive Gateway, so dass eine gemeinsame Internetverbindung über diesen Rechner genutzt werden kann.
  Standard: automatisch
  Empfehlung: deaktiviert
  System: Windows XP
  Konsequenz bei deaktiviertem Dienst: Netzwerkdienste wie die gemeinsame Nutzung von Internetverbindungen, Namensauflösung, Adressierung und Windows-Firewall Schutz sind nicht mehr verfügbar.

- Windows-Verwaltungsinstrumentation
  Grundlegend werden durch diesen Dienst Systemverwaltungsinformationen angezeigt. Unter Windows XP mit SP 1 ist dieser Dienst nicht erforderlich. Mit Windows XP SP 2 wird der Dienst für das Sicherheitscenter und die Windows-Firewall benötigt, sofern diese Komponenten vom Benutzer gewünscht sind. Auf alle Fälle brauchen wir diesen Dienst, damit wir die Abhängigkeiten der Dienste untereinander einsehen können.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP

- Windows-Zeitgeber
  Dieser Systemdienst verwaltet die Datums- und Uhrzeitsynchronisierung auf allen in einem Windows -Netzwerk ausgeführten Computern. Dieser Dienst verwendet das Network Time Protocol (NTP) für die Synchronisation von Computeruhren. In einer Einzelplatzumgebung benötigen wir diesen Dienst nicht.
  Standard: automatisch
  Empfehlung: deaktiviert
  System: Windows 2000/XP

- WMI-Leistungsadapter
  Dieser Dienst wandelt Leistungsindikatoren in Zähler um, die von Leistungsdaten-Hilfsprogrammen über die Reverseadapter-Leistungsbibliothek verwendet werden können. Auf diese Weise kann z.B. der Sysmonitor (Sysmon) Leistungszähler verwenden, die auf dem Computer angezeigt werden können.
  Standard: automatisch
  Empfehlung: automatisch
  System: Windows 2000/XP