

Profi-Tipps: Windows-Prozesse

Nach dem Systemstart von Windows sind bereits mehr als zwanzig Prozesse aktiv. Viele davon sind überflüssig und bremsen das System unnötig aus. Manche sind sogar gefährlich.

Die Arbeitsweise von Windows basiert auf Prozessen und Diensten, die ständig im Hintergrund arbeiten. Prozesse sind aktive Programme. Windows lädt sie in den Hauptspeicher, und der Prozessor arbeitet sie ab.

Dienste sind spezielle Aufgaben, die von einem Prozess erledigt werden, zum Beispiel die Druckerwarteschlange. Der Kasten „Grundlagen: So funktionieren Prozesse und Dienste“ auf Seite 20 erklärt, wie Prozesse arbeiten.

Standardmäßig laufen rund drei Dutzend Systemprozesse. Für den Betrieb von Windows ist nur ein Teil dieser Prozesse erforderlich. Die restlichen Prozesse bremsen Ihren PC aus und stellen Sicherheitslücken dar.

Prozess-Kontrolle

Nur wenn Sie genau wissen, welche Prozesse auf Ihrem System aktiv sind, erkennen Sie die unnötigen Prozesse.

1. Process Explorer installieren

Für XP und Vista: Der Windows Task-Manager, den Sie mit [Strg Umschalt Esc] aufrufen, ist einfach zu bedienen, hat aber einen Mangel: Er verschweigt den Pfad der Prozesse. Das schützt Viren und Trojaner, die oft unter dem Namen einer Systemdatei arbeiten. Eine bessere Übersicht bietet der Process Explorer 11.04 (www.microsoft.com/germany/technet/sysinternals/utilities/ProcessExplorer.mspx, kostenlos).

Steckbrief: Profi-Tipps – Windows-Prozesse**Inhalt**■ **Prozess-Kontrolle**

- 1. Process Explorer installieren S. 18
- 2. PC-Auslastung anzeigen S. 19
- 3. Details zu Prozessen anzeigen S. 19
- 4. Prozesse schnell beenden S. 20
- 5. Prioritäten für Prozesse ändern S. 22
- 6. Task-Manager ersetzen S. 24
- 7. Svchost.exe überwachen S. 24

■ **Windows-Tuning**

- 8. Dienste-Konfiguration sichern S. 24
- 9. Test-Hardwareprofil erzeugen S. 25
- 10. Überflüssige Dienste abschalten S. 25

■ **Sicherheits-Check**

- 11. Liste der Prozesse speichern S. 25
- 12. Verdächtige Prozesse scannen S. 26
- 13. Gefährliche Prozesse identifizieren S. 26
- 14. Online-Recherche nutzen S. 28
- 15. Rootkits sicher entfernen S. 28

■ **Profi-Tipps**

- 16. System für Dual-Core-CPU's optimieren S. 28
- 17. Prozessor-Auslastung steuern S. 30
- 18. Prozess-Priorität dauerhaft reduzieren S. 30

Grundlagen:

So funktionieren Prozesse und Dienste S. 20

Process Explorer 11.04:

So nutzen Sie das Tool S. 22

Überblick:

Alle Systemprozesse von Windows XP S. 29

Kompakt

Prozesse sind aktive Programme. Windows lädt sie in den Hauptspeicher. Der Prozessor arbeitet sie ab.

Anders als der Task-Manager von Windows zeigt der kostenlose Microsoft Process Explorer 11.04 auch die Programmpfade an. Schädlinge, die wie Systemdateien heißen, lassen sich damit identifizieren.

Wenn Sie diesen Artikel gelesen haben, sind Sie in der Lage, Prozesse zu entschlüsseln und zu kontrollieren.

Weitere Infos

- www.processlibrary.com
Ausführliche Informationen zu Windows-Prozessen
- www.reger24.de/processes.php
Übersicht der wichtigen Prozesse unter Windows
- www.com-magazin.de/tipps/1433
Workshop zum Beenden defekter Programme
- www.com-magazin.de/tipps/1563
Task-Manager beim Booten automatisch starten

Software-Übersicht

Programm	Quelle	Seite
AVG Anti-Rootkit Free 1.1.0.42 (Anti-Rootkit-Tool)	www.grisoft.de	28
Avira Antivir Rescue-System-CD (Live-CD)	www.avira.de	28
Dual-Core-Optimierer 1.0 (Prozessor-Optimierer)	www.thgweb.de	28
Process Explorer 11.04 (Task-Manager)	www.microsoft.com/germany/technet/sysinternals/utilities/ProcessExplorer.msp	18
Process Tamer 2.09 (Steuert die CPU-Auslastung)	www.donationcoder.com/software/Mouser/proctamer	30
Spybot Search & Destroy 1.5.2 (Entfernt Spyware)	www.safer-networking.de	26
Windows Process Tools 1.5 (Prozess-Tools)	http://sourceforge.net/projects/winpstools	26

Alle -Programme finden Sie auf Heft-CD und -DVD in der Rubrik „Computer, Windows-Prozesse“.

halten, starten Sie den Process Explorer und drücken Sie die Tastenkombination [Strg I]. Das Fenster „System Information“ öffnet sich. Wenn Sie mit der Maus über die Grafiken fahren, sehen Sie links oben, welcher Prozess die jeweilige Systemlast verursacht (Bild A).

3. Details zu Prozessen anzeigen

Für XP und Vista: Während der Task-Manager von Windows nur wenige Informationen zu laufenden Prozessen gibt, bietet der Process Explorer umfangreiche Detailinformationen.

So geht's: Der Process Explorer hinterlegt die einzelnen Prozesse mit unterschiedlichen Farben: Neu gestartete Prozesse erscheinen grün. Prozesse, die beendet werden, sind rot markiert. Prozesse, die Sie gestartet haben, etwa ein Textverarbeitungsprogramm, haben die Farbe Violett. Dienste werden in Rosa dargestellt.

Klicken Sie mit der rechten Maustaste auf einen Prozess und wählen Sie „Properties...“. Ein Fenster mit Detailinformationen zum Prozess öffnet sich (Bild B). Im Fenstertitel steht der Name des Prozesses und – durch einen Doppelpunkt getrennt – eine ▶

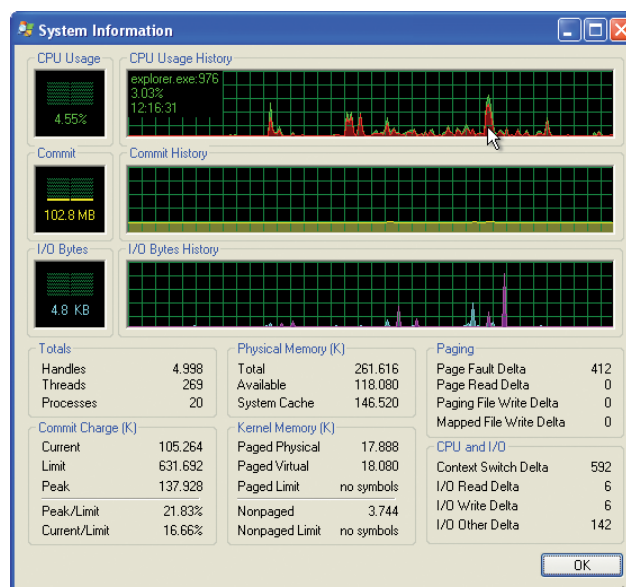
So geht's: Laden Sie das Archiv „ProcessExplorer.zip“ von der Webseite auf Ihren PC und entpacken Sie die Dateien in ein neu angelegtes Verzeichnis mit der Bezeichnung **C:\ProcessExplorer**. Starten Sie den Process Explorer mit einem Doppelklick auf „procxp.exe“. Bestätigen Sie beim ersten Start die Lizenzbedingungen mit „Agree“.

Eine Übersicht über die Bedienoberfläche des Tools gibt der Kasten „Process Explorer 11.04: So nutzen Sie das Tool“ auf Seite 22.

2. PC-Auslastung anzeigen

Für XP und Vista: Wenn Sie die PC-Auslastung stets im Blick haben, erkennen Sie fehlerhafte Prozesse.

So geht's: Um detaillierte Informationen zur Prozessor- und Speicherauslastung zu er-

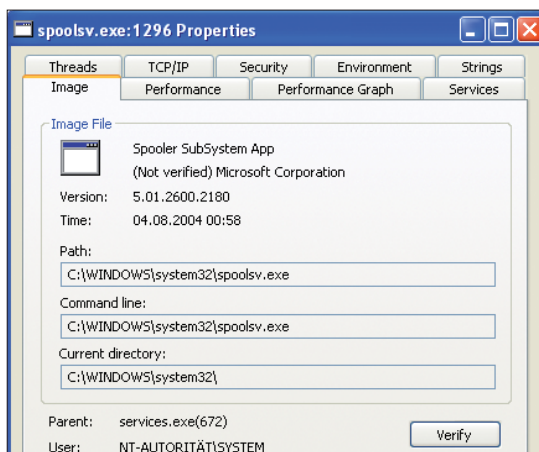


Process Explorer 11.04: Drücken Sie die Tastenkombination [Strg I]. Sie sehen dann, welcher Prozess Ihr System gerade ausbremst (Bild A)

Nummer. Dabei handelt es sich um die Prozess-ID (PID). Das ist eine eindeutige Nummer, die jedem Prozess zugeordnet ist.

Auf der Registerkarte „Image“ finden Sie unter „Path“ den Pfad zum Prozess. So lassen sich Schädlinge erkennen, die unter einem anderen Dateinamen ausgeführt werden. Ebenfalls interessant ist die bei Diensten verfügbare Registerkarte „Services“. Hier sehen Sie, welche Dienste einen Prozess nutzen. Diese Information zeigt das Tool auch an, wenn Sie im Hauptfenster den Mauszeiger über einen rosa hinterlegten Prozess bewegen.

Wenn Sie die Liste der Prozesse durchgehen, sehen Sie sicher einige, von denen Sie nicht möchten, dass sie



Process Explorer 11.04: Ein Doppelklick auf einen Prozess öffnet ein neues Fenster mit ausführlichen Informationen (Bild B)

automatisch beim Booten des PCs starten. Zum Beispiel Dienste, die Sie nicht benötigen oder die eine eventuelle Sicherheitslücke darstellen, etwa auto-

matische Software-Aktualisierungen. Um zu verhindern, dass unnötige Dienste geladen werden, ändern Sie deren Starttyp. Wie das funktioniert, erklärt Tipp 10 auf Seite 25.

Falls Ihnen ein Prozess unbekannt ist und die Informationen des Process Explorers nicht ausreichend sind, um zu beurteilen, ob es sich um einen Schädling handelt, starten Sie eine Internetsuche. Klicken Sie dazu mit der rechten Maustaste auf den Prozess und wählen Sie „Search Online ...“.

4. Prozesse schnell beenden

Für XP und Vista: Fehlerhafte Programme lassen sich oft nicht mehr über deren Bedienoberfläche beenden. Hier hilft der Process Explorer weiter. ▶

Grundlagen: So funktionieren Prozesse und Dienste

Die Arbeitsweise von Windows basiert auf einer Reihe von Prozessen und Diensten, die ständig im Hintergrund arbeiten. Sie liegen im Hauptspeicher und werden vom Prozessor abgearbeitet. So funktioniert Windows.

Prozesse sind aktive Programme. Windows lädt sie in den Hauptspeicher, und der Prozessor arbeitet sie ab. Es gibt drei Arten von Prozessen: Steuerprogramme für Dienste, System-Tray-Programme und Anwendungen. Welche Prozesse aktiv sind, zeigt der Task-Manager. Sie öffnen ihn mit den Tasten [Strg Umschalt Esc].

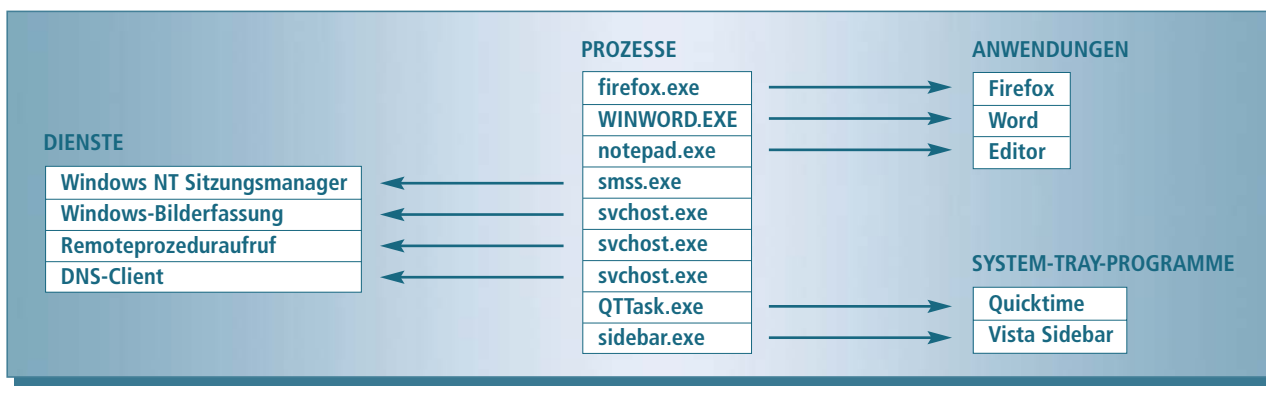
Dienste: Ein Dienst ist eine bestimmte Aufgabe, die von einem Prozess erledigt wird. So führt etwa der Dienst „spoolsv.exe“ die Druckerwarteschlange aus. Jeder Dienst besitzt einen Anzeigenamen, etwa „DNS-

Client“, und einen Dienstenamen, zum Beispiel „Dnscache“. Die meisten Prozesse werden vom Prozess „svchost.exe“ gesteuert. Welche Dienste wann ausgeführt werden, bestimmt der Anwender in der Dienstverwaltung.

System-Tray-Programme: Diese Prozesse erfüllen nur den Zweck, ein Symbol in die System-Tray-Leiste neben der Uhr in der Taskleiste abzulegen. Ein Doppelklick auf das Symbol startet ein Programm, etwa die Konfiguration eines Virencanners. Diese Prozesse starten automatisch beim

Systemstart und lassen sich über das Systemkonfigurationsprogramm deaktivieren. Sie starten das Tool, indem Sie [Windows R] drücken, msconfig eingeben und mit „OK“ bestätigen. Die System-Tray-Programme finden Sie in der Registerkarte „Systemstart“.

Anwendungen: Die vom Anwender gestarteten Programme wie Word oder Firefox werden wie alle Prozesse im Task-Manager mit den Namen der Programmdatei angezeigt. So heißt etwa Firefox im Task-Manager „firefox.exe“.



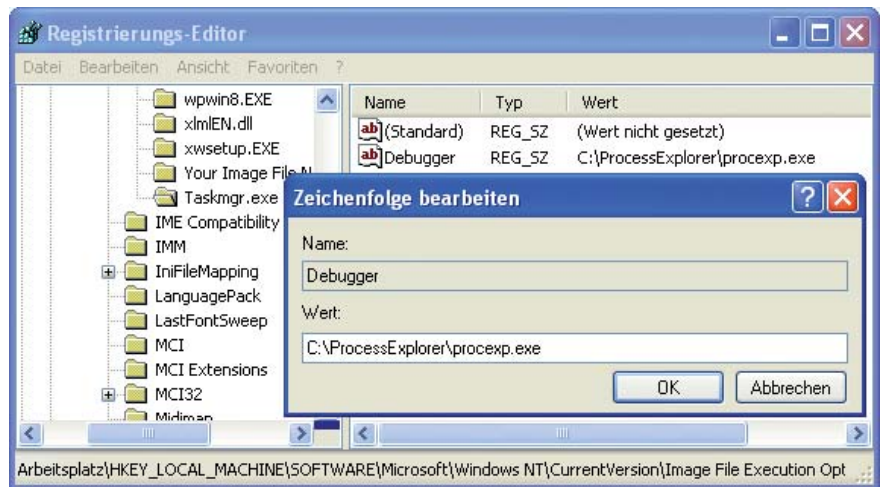
So geht's: Klicken Sie im Hauptfenster des Process Explorers mit der rechten Maustaste auf einen Prozess und wählen Sie „Kill Process, Ja“. Der Prozess wird rot hinterlegt und gelöscht.

Achtung: Damit werden Prozesse sofort und ohne Nachfrage beendet. Ungespeicherte Daten können verloren gehen. Zudem sind einige Prozesse für ein funktionierendes System unerlässlich und sollten nicht beendet werden. Welche Prozesse Sie nicht beenden sollten, lesen Sie im Kasten „Überblick: Alle Systemprozesse von Windows XP“ ab Seite 29.

Weitere Informationen, wie sich hängende Programme automatisch beenden lassen, lesen Sie im Internet unter www.com-magazin.de/tipps/1433.

5. Prioritäten für Prozesse ändern

Für XP und Vista: Mit dem Process Explorer lässt sich auch die Priorität eines Prozesses ändern. Je höher die Priorität eines Prozesses, desto mehr CPU-Zeit bekommt er zugewiesen.



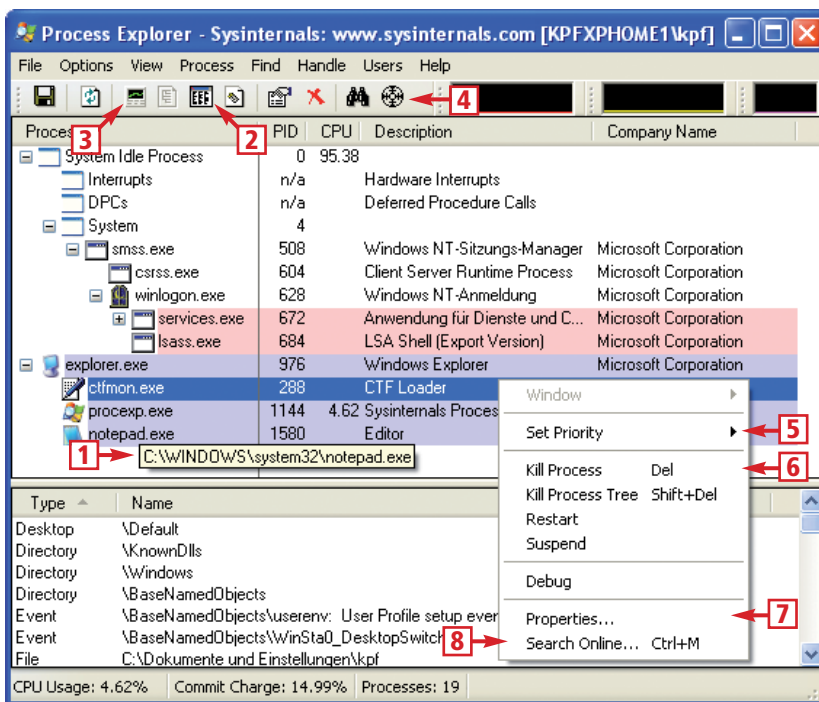
Zeichenfolge bearbeiten: Eine Registry-Manipulation ersetzt den Windows Task-Manager dauerhaft durch ein alternatives Programm (Bild C)

So geht's: Windows XP und Vista kennen sechs Prioritätsstufen: „Niedrig“, „Niedriger als normal“, „Normal“, „Höher als normal“, „Hoch“ sowie „Echtzeit“. Die meisten Prozesse laufen mit der Priorität „Normal“. Einige wichtige Prozesse, wie der Task-Manager, laufen mit der Priorität „Hoch“.

Wenn ein Programm sich zu sehr in den Vordergrund drängt oder das System ausbremst, setzen Sie dessen Priorität herunter: Klicken Sie mit der rechten Maustaste auf den Prozess und wählen Sie „Set Priority, Below Normal: 6“. Wenn ein Programm zu langsam arbeitet, wählen Sie die Priorität „Abo- ▶

Process Explorer 11.04: So nutzen Sie das Tool

Das Programm Process Explorer 11.04 zeigt übersichtlich alle aktiven Prozesse auf dem System an. Zudem bietet es umfangreiche Informationen zur Systemauslastung.



- 1 Pfad zum Prozess**
Wenn Sie den Mauszeiger über einen Prozess bewegen, erscheint der Pfad
- 2 Detailinformationen**
Die Schaltfläche blendet weitere Details zum markierten Prozess ein
- 3 Systeminformationen**
Die Schaltfläche öffnet ein Fenster mit der CPU- und Speicherauslastung
- 4 Prozess ermitteln**
Wenn Sie darauf klicken und das Symbol über ein Windows-Fenster ziehen, wird der zugehörige Prozess markiert
- 5 Priorität ändern**
Der Kontextmenü-Eintrag ändert die Priorität für den markierten Prozess
- 6 Prozess stoppen**
Diese Funktion beendet einen Prozess
- 7 Eigenschaften**
Der Kontextmenü-Eintrag öffnet das Eigenschaften-Fenster eines Prozesses
- 8 Suche im Internet**
Diese Funktion startet eine Websuche nach einem Prozess

ve Normal: 10" – damit wird der Prozess beschleunigt. Die Einstellungen „High: 13" und „Realtime: 24" sollten Sie vermeiden, da sie zu Abstürzen führen.

6. Task-Manager ersetzen

Für XP und Vista: Der Windows Task-Manager hat einen beschränkten Funktionsumfang. So ersetzen Sie ihn dauerhaft durch den Process Explorer.

So geht's: Öffnen Sie den Registrierungs-Editor, indem Sie [Windows R] drücken, `regedit` eingeben und mit „OK" bestätigen. Markieren Sie den Schlüssel „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options".

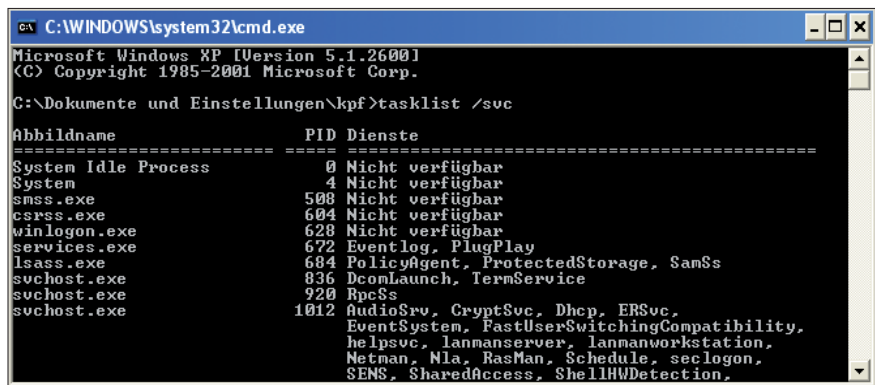
Wählen Sie „Bearbeiten, Neu, Schlüssel" und ersetzen Sie „Neuer Schlüssel #1" durch `Taskmgr.exe`. Markieren Sie „Taskmgr.exe" und wählen Sie „Bearbeiten, Neu, Zeichenfolge". Ersetzen Sie „Neuer Wert #1" durch `Debugger`. Klicken Sie doppelt auf „Debugger" und geben Sie unter „Wert" den Pfad `C:\ProcessExplorer\procexp.exe` ein (Bild C). Fortan startet mit [Strg Umschalt Esc] der Process Explorer.

Um die Änderung rückgängig zu machen, löschen Sie in der Registry den Schlüssel „Taskmgr.exe".

Wie Sie den Process Explorer bei jedem Systemstart automatisch starten, lesen Sie im Internet unter www.com-magazin.de/tips/1563.

7. Svchost.exe überwachen

Für XP und Vista: Der am häufigsten genutzte Prozess ist „svchost.exe". Er wird von Diensten gestartet, die auf DLL-Dateien beruhen. Der Process Explorer listet die Bezeichnung „svchost.exe" stets mehrfach auf. Das liegt daran, dass die den Prozess aufrufenden Dienste in Gruppen aufgeteilt sind. Jede Gruppe startet jeweils eine Instanz dieses Prozesses.



Eingabeaufforderung: Der Befehl `tasklist /svc` gibt eine Liste der mit der Datei „svchost.exe" verbundenen Dienste aus (Bild D)

So geht's: Fahren Sie im Hauptfenster des Process Explorers mit dem Mauszeiger über eine Instanz von „svchost.exe". Ein Tooltip zeigt die Dienste an, welche die Instanz gestartet haben.

Auch ohne den Process Explorer lassen sich die Dienste anzeigen: Nutzen Sie dazu das Tool „tasklist.exe". Bei Windows XP Home steht es nicht zur Verfügung. Besorgen Sie sich in diesem Fall eine Installations-CD von Windows XP Professional und öffnen Sie die Kommandozeile, indem Sie [Windows R] drücken, `cmd` eingeben und mit „OK" bestätigen. Geben Sie folgenden Befehl ein:

```
1 expand <Laufwerk>:\i386\tasklist.exe -C:\Windows\system32\tasklist.exe
```

Ersetzen Sie <Laufwerk> durch den Laufwerkbuchstaben des CD-Laufwerks. Geben Sie nun den Befehl `tasklist /svc` ein. Das Tool zeigt die Instanzen von „svchost.exe" und deren Dienste an (Bild D).

Windows-Tuning

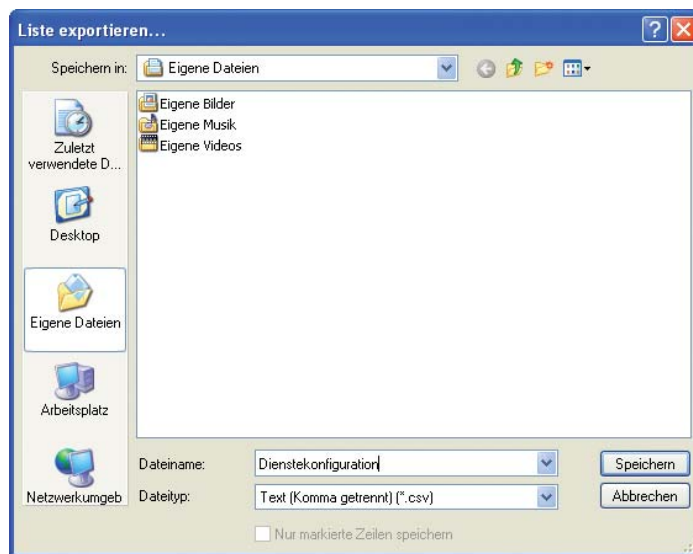
Viele Prozesse sind für den Betrieb des PCs nicht nötig und verlangsamen das System. Zudem vergrößert jeder an das Internet gekoppelte Prozess das Risiko, dass ein Schädling eindringt.

8. Dienste-Konfiguration sichern

Für XP und Vista: Bevor Sie den Starttyp einzelner Dienste ändern, sichern Sie eine Liste der aktuellen Konfiguration.

So lassen sich die Einstellungen wiederherstellen.

So geht's: Öffnen Sie die Dienstverwaltung, indem Sie [Windows R] drücken, `services.msc` eingeben und mit „OK" bestätigen. Markieren Sie „Dienste (Lokal)" und wählen Sie „Aktion, Liste exportieren...". Legen Sie einen Speicherort fest und vergeben Sie einen Namen wie **Dienstekonfiguration**. Als „Dateityp" wählen Sie „Text (Komma getrennt) (*.csv)" (Bild E). Die Datei lässt sich mit einer Tabellenkalkulation wie Excel öffnen und ausdrucken.



Liste exportieren: In der Dienstverwaltung lässt sich die aktuelle Konfiguration der Dienste sichern. Wählen Sie als Dateityp „Text (Komma getrennt) (*.csv)" (Bild E)

9. Test-Hardwareprofil erzeugen

Für XP: Bevor Sie die Konfiguration der Dienste ändern, legen Sie ein neues Hardwareprofil an, mit dem Sie die Änderungen vorab testen.

So geht's: Öffnen Sie die Systemeigenschaften mit [Windows Pause]. Wählen Sie „Hardware, Hardwareprofile, Kopieren“. Weisen Sie dem neuen Hardwareprofil einen Namen zu, etwa **Profil · nur · mit · wichtigen · Diensten**. Klicken Sie jeweils doppelt auf „Profil 1 (Aktuell)“ und „Profil nur mit wichtigen Diensten“ und aktivieren Sie „Dieses Profil beim Windows-Start immer einschließen“.

Starten Sie den PC neu und wählen Sie beim Hochfahren mit den Pfeil-Tasten das Profil „Profil nur mit wichtigen Diensten“. Nehmen Sie wie im folgenden Tipp 10 beschrieben die Änderungen an den Diensten vor und testen Sie, ob der PC damit problemlos arbeitet. Wenn Sie keine Störungen feststellen, lassen Sie den PC fortan automatisch mit dem neuen Profil starten.

Öffnen Sie dazu erneut die Konfiguration der Hardwareprofile und markieren Sie das „Profil nur mit wichtigen Diensten“. Klicken Sie rechts auf den Pfeil, der nach oben zeigt, um das neue Profil an die erste Stelle zu setzen (Bild F).

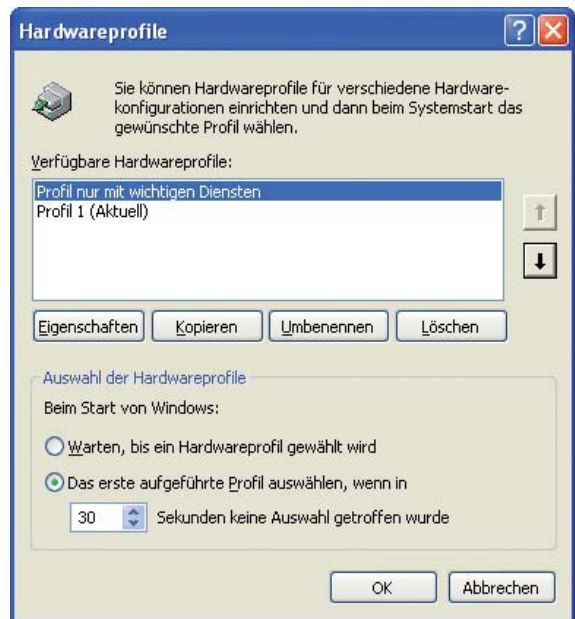
Wenn Sie zu einem späteren Zeitpunkt wieder die ursprüngliche Dienste-Konfiguration nutzen wollen, setzen Sie das „Profil 1“ an die erste Stelle und starten den PC neu.

10. Überflüssige Dienste abschalten

Für XP und Vista: Windows startet beim Hochfahren Dienste, die viele Nutzer nicht benötigen. Schalten Sie sie daher ab.

So geht's: Starten Sie die Dienstverwaltung, indem Sie [Windows R] drücken, **services.msc** eingeben und mit „OK“ bestätigen (Bild G). Wenn Sie doppelt auf einen Dienst klicken, etwa auf „DNS-Client“, öffnet sich dessen Eigenschaften-Fenster. Darin sehen Sie auf der Registerkarte „Allgemein“ den Dienstnamen, in diesem Beispiel „Dnscache“, den Anzeigenamen, eine kurze Beschreibung sowie den Pfad zur EXE-Datei. Wenn der Dienst einer Service-Gruppe angehört, steht dort **C:\WINDOWS\System32\svchost.exe -k <Gruppe>**. Beim Dienst „DNS-Client“ heißt die Gruppe „NetworkService“.

Im Pulldown-Menü neben „Starttyp“ stehen drei Modi zur Verfügung: Ein „Manuell“ gestarteter Dienst wird vom System nur bei Bedarf geladen. Manuell startende Dienste lassen sich aber auch vom Anwender aktivieren: Markieren Sie in der Dienstverwaltung einen Dienst und klicken Sie links auf



Hardwareprofile: Mit einem neuen Profil „Profil nur mit wichtigen Diensten“ testen Sie gefahrlos die geänderte Konfiguration (Bild F)

„Den Dienst starten“. Der Starttyp „Deaktiviert“ bedeutet, dass ein Dienst nicht gestartet werden kann – weder vom System noch vom Benutzer. Mit dem Starttyp „Automatisch“ wird ein Dienst automatisch beim Systemstart geladen.

Vorsicht: Falls Sie wichtige Dienste deaktivieren, läuft Windows nicht mehr rund. Um einen Dienst abzuschalten, wählen Sie den Starttyp „Manuell“. So kann das System einen Dienst bei Bedarf selbst starten. Im Kasten „Überblick: Alle Systemprozesse von Windows XP“ ab Seite 29 finden Sie eine Übersicht über alle Dienste und eine Empfehlung für den Starttyp.

Sicherheits-Check

Keylogger, Passwort-Sniffer und trojanische Pferde setzen Prozesse in Gang, die im Hintergrund agieren und mit Hackern Kontakt aufnehmen. Falls sich ein Schädling einnistet, lässt er sich nach einem Neustart in der Prozessliste identifizieren.

11. Liste der Prozesse speichern

Für XP und Vista: Die im Task-Manager angezeigte Prozessliste enthält viele Einträge. Damit Sie trotzdem die ►



Dienste: In der Dienstverwaltung von Windows XP und Vista legen Sie fest, welche Dienste beim Systemstart automatisch gestartet werden (Bild G)

Standardprozesse von neuen, möglicherweise schädlichen Prozessen unterscheiden können, sollten Sie die Liste regelmäßig speichern. Dabei unterstützen Sie die Windows Process Tools 1.5 (<http://sourceforge.net/projects/winpstools>, kostenlos).

So geht's: Entpacken Sie von der Heft-CD oder -DVD unter „Computer, Windows-Prozesse“ das Archiv „winpstools-1.5.zip“ in das neue Verzeichnis **C:\Windows-Prozesse**. Öffnen Sie die Eingabeaufforderung, indem Sie [Windows R] drücken, **cmd** eingeben und mit „OK“ bestätigen. Wenn Sie den Befehl **C:\Windows-Prozesse\wps** eingeben, zeigt Ihnen das Tool eine Liste der aktiven Prozesse an.

Um die Liste zu speichern, erstellen Sie eine Batch-Datei, welche die Ausgabe in eine Textdatei umleitet: Starten Sie den Windows-Editor und schreiben Sie folgende Befehle in die Textdatei:

```
1 echo %date% >> prozessliste.txt
2 echo %time% >> prozessliste.txt
3 wps >> prozessliste.txt
4 echo ----- >> prozessliste.txt
```

Speichern Sie die Datei unter dem Namen **prozessliste.cmd** im Ordner „C:\Windows-Prozesse“. Wählen Sie im Dialogfenster „Speichern unter“ als „Dateityp“ die Einstellung „Alle Dateien“.

Führen Sie das Batch-Programm aus, indem Sie in dem Ordner „C:\Windows-Prozesse“ doppelt auf „prozessliste.cmd“ klicken. Das Tool legt im selben Ordner die Datei „prozessliste.txt“ mit einer Liste der Prozesse ab (Bild H).

12. Verdächtige Prozesse scannen

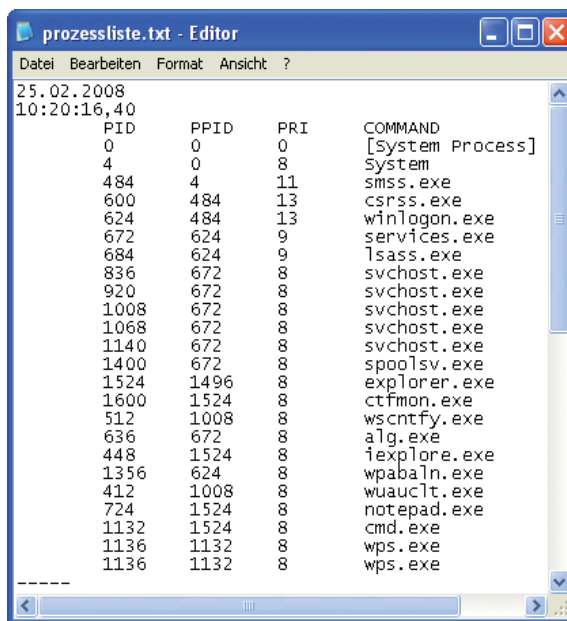
Für XP und Vista: Falls Ihnen ein Prozess verdächtig erscheint, gibt es eine einfache Möglichkeit, ihn zu prüfen: Lassen Sie die Programmdatei online checken.

So geht's: Ermitteln Sie die Programmdatei zum Prozess. Klicken Sie dazu im Process Explorer doppelt auf den Prozess und wählen Sie „Image“. Markieren Sie unter „Path“ mit der Maus den Pfad und kopieren Sie ihn mit [Strg C] in die Zwischenablage.

Öffnen Sie im Browser die Adresse **www.virus-total.com** und klicken Sie unter „Eine Datei hochladen“ auf das Textfeld. Drücken Sie [Strg V] und bestätigen Sie mit „Senden der Datei“. Sobald die Datei mit den Signaturen von 32 Virensclannern überprüft wurde, erscheint das Ergebnis (Bild I).

13. Gefährliche Prozesse identifizieren

Für XP und Vista: Wenn es darum geht, bereits aktive Computerschädlinge zu erkennen, benötigen Sie meist ein Anti-Spyware-Tool.



Editor mit „prozessliste.txt“: Die Windows Process Tools 1.5 und ein Batch-Programm speichern eine Liste der Prozesse (Bild H)

So geht's: Installieren Sie Spybot Search & Destroy 1.5.2 (www.safer-net-working.de, kostenlos). Sie finden das Tool auf Heft-CD und -DVD unter „Computer, Windows-Prozesse“. Nach der Installation startet der Konfigurationsassistent. Bei „Nach Updates suchen“ fahren Sie fort mit „Weiter“. Klicken Sie auf „Programm benutzen“ und „Nach Updates suchen, Fortfahren“. Klicken Sie mit der rechten Maustaste in das Fenster mit den Updates und wählen Sie „Alle wählen“. Fahren Sie fort mit „Herunterladen“.

Starten Sie Windows neu im abgesicherten Modus. Drücken Sie dazu während des Bootens mehrmals [F8], bis die erweiterten Startoptionen erscheinen, und wählen Sie „Abgesicherter Modus“. Melden Sie sich unter Ihrem Benutzernamen an, bestätigen Sie mit „Ja“ und starten Sie Spybot Search & Destroy. Klicken Sie auf „Überprüfen“ (Bild J). Das Tool erstellt eine Liste der gefundenen Schädlinge. Um diese zu entfernen, wählen Sie „Markierte Probleme beheben“.



Virus Total: Die Webseite überprüft verdächtige Prozesse mit den Signaturen von 32 Virensclannern (Bild I)

14. Online-Recherche nutzen

Für XP und Vista: Falls ein Anti-Spyware-Tool einen Schädling nicht entfernen kann, sind spezielle Maßnahmen nötig.

So geht's: Starten Sie eine Suchmaschine wie Google und forschen Sie nach dem Namen des Schädling oder dem Prozessnamen. Nehmen Sie auch Suchseiten von Virenschutzanbietern zu Hilfe, etwa unter <http://secunia.com/search>. Auch in zahlreichen Internetforen tauschen Anwender ihre Erfahrungen über Schädlinge aus. Alle Webforen enthalten Archive mit sämtlichen Einträgen der Vergangenheit. Sie zu durchforsten, lohnt sich. Die besten Online-Foren hierfür sind: Hijackthis.de (<http://forum.hijackthis.de>), Trojaner-Board (www.trojaner-board.de), Protecus Security (<http://board.protecus.de>) sowie Computerhilfen (www.computerhilfen.de).

15. Rootkits sicher entfernen

Für XP: Rootkits sind eine tückische Variante von Schädlingen. Mit manipulierten Systemdateien blenden sie sich aus dem Task-Manager aus.

So geht's: Das AVG Anti-Rootkit Free 1.1.0.42 (www.grisoft.de, kostenlos) entfernt Rootkits (Bild K). Sie finden das



Spybot Search & Destroy 1.5.2: Ein Klick auf „Überprüfen“ startet die Suche nach schädlichen Programmen. Falls Schädlinge gefunden werden, entfernen Sie sie mit „Markierte Probleme beheben“ (Bild J)

Tool auf Heft-CD und -DVD unter „Computer, Windows-Prozesse“. Installieren Sie es, booten Sie den PC neu und starten Sie das Tool.

Starten Sie die Suche mit „Perform in-depth search“. Markieren Sie die Einträge, die zu Rootkits gehören. Wenn Sie sich nicht sicher sind, welche das sind, starten Sie eine Recherche wie in

Tipp 14 beschrieben. Klicken Sie dann auf „Remove selected items“ und markieren Sie „I have read and understood the warning information...“. Bestätigen Sie mit „OK“ und schließen Sie nach dem Neustart das Fenster mit „Close“.

Wenn AVG Anti-Rootkit Free die Schädlinge nicht entfernen kann, scannen Sie den PC zusätzlich mit der Live-CD Avira Antivir Rescue-System-CD (www.avira.de, kostenlos).

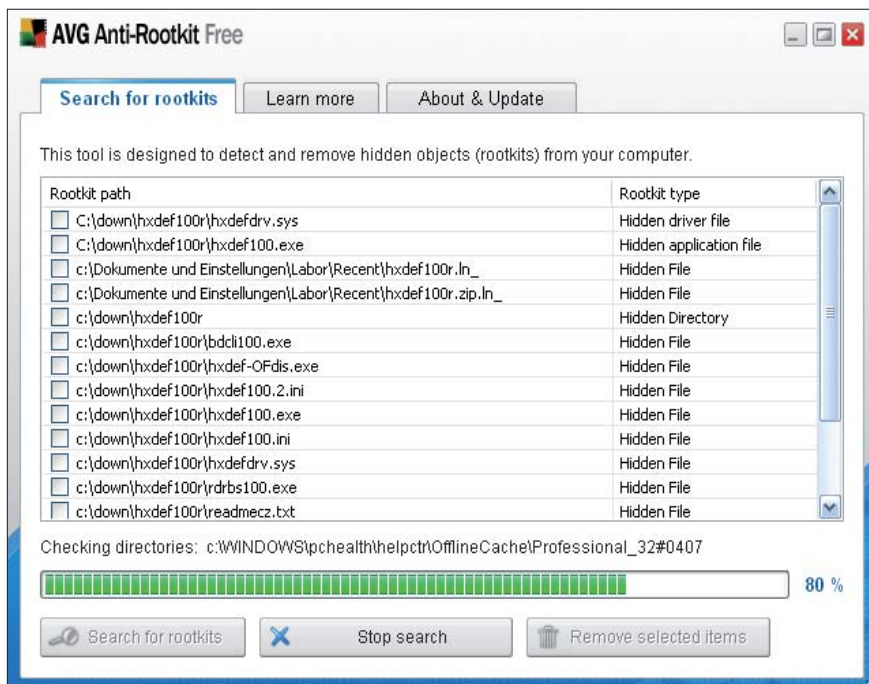
Sie finden das ISO-Image der Rescue-CD auf Heft-CD und -DVD unter „Computer, Windows-Prozesse“. Eine Beschreibung dazu lesen Sie im Artikel „Neue Gefahr: Rootkits“ auf Seite 70 im Abschnitt „PC mit Live-CD reinigen“.

Profi-Tipps

Spezialtricks erhöhen die PC-Leistung, etwa wenn Sie einen Computer mit Dual-Core-Prozessor nutzen.

16. System für Dual-Core-CPUs optimieren

Für XP: Ältere Software nutzt nur einen Prozessor. Auf einem Multiprozessor-System bringen diese Programme weniger Leistung, und der Rest des Systems wird unnötig ausgebremst. Software, die nur eine CPU nutzt, erkennen



AVG Anti-Rootkit Free 1.1.0.42: Das Tool durchsucht den PC auf Rootkits und entfernt diese (Bild K)

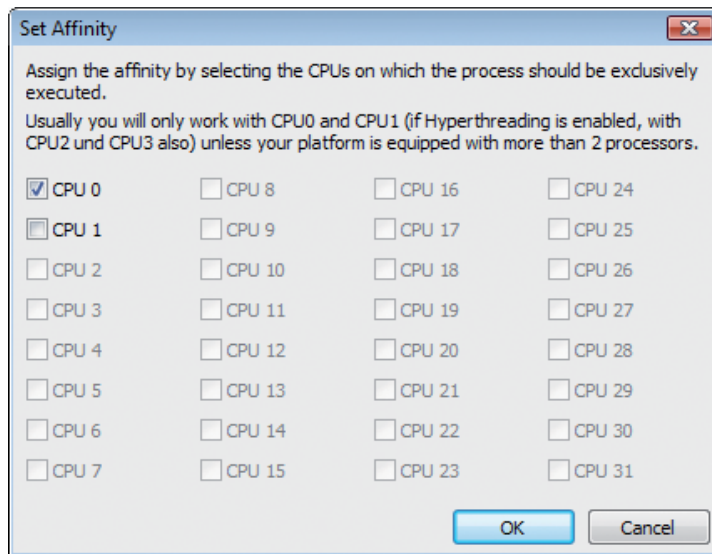
Überblick: Alle Systemprozesse von Windows XP – Teil I (Fortsetzung Seite 31)

Die Übersicht enthält alle Systemprozesse von Windows XP. Die Empfehlungen für den Starttyp gelten für Standard-PCs mit Internetzugang. Die Firewall sollte alle Prozesse außer „explorer.exe“, „lsass.exe“ und „svchost.exe“ blocken.

Dateiname	Prozessname	Standardpfad	Empfehlung	Bei Firewall-Anfragen	Beschreibung
alg.exe	Gateway-Dienst auf Anwendungsebene	C:\WINDOWS\system32\alg.exe	In Dienstverwaltung deaktivieren	Blocken	Kontrolliert den Internetzugriff, sobald mehrere PCs den Internetanschluss eines anderen Computers nutzen. Bei anderen Anschlussformen – direkt oder via Router – nicht nötig
cisvc.exe	Indicedienst	C:\WINDOWS\system32\cisvc.exe	In Dienstverwaltung auf „Manuell“ einstellen	Blocken	Indiziert Dateiinhalte auf dem PC und auf Netzlaufwerken. Vorteil: schnelle Suche. Problem: bremst den PC
clipsrv.exe	Ablagemappe	C:\WINDOWS\system32\clipsrv.exe	In Dienstverwaltung deaktivieren	Blocken	Tauscht Inhalte der Zwischenablage im Heimnetz. Gilt als unsicher
csrss.exe	Client-Server-Runtime-Subsystem	C:\WINDOWS\system32\csrss.exe	Nicht beenden	Blocken	Steuert die Kommunikation von Windows-Prozessen untereinander. Erforderliche Basiskomponente
ctfmon.exe	Alternative Benutzereingabe	C:\WINDOWS\system32\ctfmon.exe	In Msconfig unter „Systemstart“ beenden	Blocken	Ermöglicht Sprach- und Schrifterkennung sowie die Gebietschemaeiste. Nur nötig für Sprach- und Schrifterkennung mit Software von Microsoft
dllhost.exe	COM-Modul für DLL-gestützte COM-Objekte	C:\WINDOWS\system32\dllhost.exe	Nicht beenden	Blocken	Steuert die beiden Dienste „COM+Systemanwendung“ und „MS Software Shadow Copy Provider“. Erforderliche Basiskomponente
dmadmin.exe	Verwaltungsdienst für Verwaltung logischer Datenträger	C:\WINDOWS\system32\dmadmin.exe	Nicht beenden	Blocken	Startet beim Öffnen der Datenträgerverwaltung. Erforderliche Basiskomponente
explorer.exe	Windows-Explorer	C:\WINDOWS\system32\explorer.exe	Beenden, wenn eine andere Oberfläche eingesetzt wird	Zulassen	Steuert die Bedienoberfläche von Windows. Wiederholter Aufruf öffnet ein Fenster des Windows-Dateimanagers. Internetzugriff ist zum Öffnen von FTP-Verzeichnissen nötig
imapi.exe	IMAPI-CD-Brenn-COM-Dienste	C:\WINDOWS\system32\imapi.exe	In Dienstverwaltung deaktivieren	Blocken	Ermöglicht es, CDs mit dem Windows-Explorer zu brennen. Führt in vielen Fällen zu Konflikten mit anderen Brennprogrammen
Leerlaufprozess	Leerlaufprozess	–	Nicht beenden	Blocken	Reserviert freie CPU-Kapazität für weitere Prozesse. Erforderliche Basiskomponente
locator.exe	RPC-Locator	C:\WINDOWS\system32\locator.exe	Nicht beenden	Blocken	Verwaltet die Datenbank für den RPC-Namensdienst. RPC (Remote Procedure Call) ermöglicht den Datenaustausch von Prozessen übers Netzwerk
lsass.exe	Lokaler Sicherheitsdienst	C:\WINDOWS\system32\lsass.exe	Nicht beenden	Zulassen	Verwaltet zum Beispiel die Kontodaten der Benutzer. Erforderliche Basiskomponente
mnmsrvc.exe	NetMeeting-Remotedesktop-Freigabe	C:\WINDOWS\system32\mnmsrvc.exe	In Dienstverwaltung deaktivieren	Blocken	Ermöglicht es, einen anderen PC mit der Software Netmeeting fernzusteuern. Gilt als unsicher
msdtc.exe	Distributed Transaction Coordinator	C:\WINDOWS\system32\msdtc.exe	Nicht beenden	Blocken	Vermittelt zwischen datenbankgestützten Programmen und SQL-Datenbanken; unter Umständen für den Betrieb einer installierten Software erforderlich
msiexec.exe	Windows-Installer	C:\WINDOWS\system32\msiexec.exe	Nicht beenden	Blocken	Startet beim Installieren einer Software per Doppelklick auf eine Datei mit der Endung MSI
msmsgs.exe	Windows Messenger	C:\Programme\Messenger\msmsgs.exe	In Msconfig unter „Systemstart“ deaktivieren	Blocken	Wird standardmäßig beim Systemstart geladen
netdde.exe	Net-DDE-Dienst und Netzwerk-DDE-Serverdient	C:\WINDOWS\system32\netdde.exe	In Dienstverwaltung deaktivieren	Blocken	Antiquierter Netzwerkdienst, steuert den Datenaustausch von DDE-Anwendungen wie der Ablagemappe; sehr selten auch für den Betrieb von Software anderer Hersteller erforderlich
rsvp.exe	QoS-RSVP	C:\WINDOWS\system32\rsvp.exe	In Dienstverwaltung deaktivieren	Blocken	Reserviert für Video-Streams und andere Anwendungen Übertragungskapazitäten im Netzwerk. Im Heimnetz unnötig

Sie im Windows Task-Manager: Die unter „Systemleistung“ angezeigte CPU-Auslastung bleibt stets unter 50 Prozent.

So geht's: Entpacken Sie den Dual-Core-Optimierer 1.0 (THG Task Assignment Manager, www.thgweb.de, kostenlos) von der Heft-CD oder -DVD unter „Computer, Windows-Prozesse“ in den neuen Ordner `C:\THG`. Starten Sie das Tool mit einem Doppelklick auf „TaskAssign.exe“. Markieren Sie unter „Select Application and Assign“ das Programm, das nur einen Prozessor nutzt, und wählen Sie „Assign task affinity to a certain CPU“. Ordnen Sie den Prozess einem Prozessor der CPU zu (Bild L). Damit Sie dies nicht nach jedem Programmstart einstellen müssen, legen Sie ein Profil an: Wechseln Sie auf „Application Profiles“. Klicken Sie auf „Browse“ und markieren Sie die Programmdatei, die schneller laufen soll. Klicken Sie auf „Öffnen, Add“. Das Zuweisungsmenü



Dual-Core-Optimierer 1.0: Weisen Sie mit dem Tool älterer Software nur einen Prozessorkern zu, um mehr Leistung für andere Anwendungen zu erhalten (Bild L)

erscheint. Setzen Sie einen Haken bei der CPU, der Sie die Software zuordnen möchten. Die Zuordnung zu einem Prozessorkern funktioniert jedoch nur, solange der Dual-Core-Optimierer läuft.

Mehr Tipps zu Dual-Core-CPU stehen im Artikel „Windows XP für Dual Core optimieren“ in com! 12/2007 ab Seite 22. Den Artikel finden Sie als PDF-Datei auf Heft-CD und -DVD unter „Computer, Windows-Prozesse“.

17. Prozessor-Auslastung steuern

Für XP: Ein Prozess, der die CPU auslastet, bremst andere Anwendungen. Das führt dazu, dass der PC sich kaum noch bedienen lässt. Durch eine Kontrolle der CPU-Auslastung vermeiden Sie dies.

So geht's: Das Tool Process Tamer 2.09 (www.donationcoder.com/Software/Mouser/proctamer, kostenlos) drosselt Prozesse, sobald sie die CPU zu stark belasten. Installieren Sie das Programm von der Heft-CD oder -DVD unter „Computer, Win-

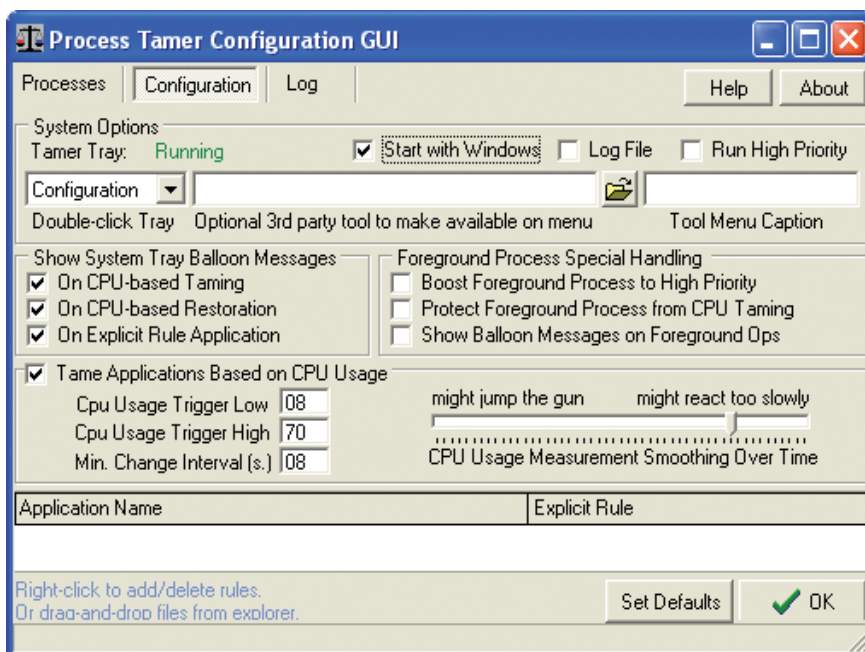
dows-Prozesse“ und starten Sie es. Klicken Sie auf „Configuration“. Aktivieren Sie „Start with Windows“, wenn Sie die Steuerung dauerhaft installieren möchten (Bild M). Fortan ändert das Tool für Prozesse, die mehr als 70 Prozent Last benötigen, die Priorität auf „Niedrig“. Erst wenn die Leistungsaufnahme unter diesen Wert sinkt, setzt Process Tamer die Priorität auf „Normal“.

18. Prozess-Priorität dauerhaft reduzieren

Für XP: Rechenintensive Programme können den PC lahmlegen. Beim Aufruf solcher Tools sollten Sie deren Prozesspriorität verringern. Die Programme laufen zwar langsamer, beeinträchtigen andere Anwendungen aber weniger.

So geht's: Legen Sie auf dem Desktop eine Verknüpfung für die Anwendung an, indem Sie das Programmsymbol aus dem Startmenü auf den Desktop schieben. Klicken Sie mit der rechten Maustaste auf die Verknüpfung und wählen Sie „Eigenschaften“. Unter „Verknüpfung“ setzen Sie den Cursor im Textfeld neben „Ziel“ ganz links und geben vor dem Programmpfad `cmd /c start /low` ein. Bestätigen Sie mit „OK“.

Konstantin Pfliegl/Klaus Plessner
computer@com-magazin.de



Process Tamer 2.09: Die Einstellung „Start with Windows“ sorgt dafür, dass das Tool automatisch mit Windows startet und stets die Prozessorlast überprüft (Bild M)

Überblick: Alle Systemprozesse von Windows XP – Teil II

Dateiname	Prozessname	Standardpfad	Empfehlung	Bei Firewall-Anfragen	Beschreibung
rundll32.exe	DLL-Startprogramm	C:\WINDOWS\system32\rundll32.exe	Nicht beenden	Blocken	Führt einige System-DLL-Dateien als Programm aus. Startet zum Beispiel beim Öffnen von Desktop-Elementen wie „Eigenschaften von Uhr ...“
scardsvr.exe	Smartcard	C:\WINDOWS\system32\SCardSvr.exe	In Dienstverwaltung deaktivieren	Blocken	Steuert Smartcard-Lesegerät; nur bei Anschluss von Lesegeräten erforderlich
sessmgr.exe	Sitzungsmanager für Remotedesktophilfe	C:\WINDOWS\system32\sessmgr.exe	In Dienstverwaltung deaktivieren	Blocken	Ermöglicht Fernsteuerung über „Remotedesktop“. Wird selten genutzt, weil Fernsteuerungs-Software wie VNC besser ist
smlogsvc.exe	Leistungsdatenprotokolle und Warnungen	C:\WINDOWS\system32\smlogsvc.exe	Nicht beenden	Blocken	Sammelt Protokolldaten von PCs im Netz; unter Umständen für installierte Software erforderlich
smss.exe	Windows NT Sitzungsmanager	C:\WINDOWS\system32\smss.exe	Nicht beenden	Blocken	Wird vom Systemprozess gestartet und kontrolliert eine Benutzersitzung von der Anmeldung bis zur Abmeldung. Erforderliche Basiskomponente
spoolsv.exe	Druckerwarteschlange	C:\WINDOWS\system32\spoolsv.exe	Nicht beenden	Blocken	Dient als Zwischenspeicher für Druckseiten, die zum Beispiel von Word ausgegeben werden
svchost.exe	Service Host	C:\WINDOWS\system32\svchost.exe	Nicht beenden	Zulassen	Steuert verschiedene System- und Netzwerkdienste. Für jede Gruppe von Diensten startet eine eigene Instanz von svchost.exe
System	Systemdienst	–	Nicht beenden	Blocken	Fasst alle Teilprozesse beziehungsweise Threads des Windows-Kerns zusammen. Erforderliche Basiskomponente
System Idle Process	Leerlaufprozess	–	Nicht beenden	Blocken	Der englische Name für Leerlaufprozess. Erscheint zum Beispiel in der Prozessliste von Process Explorer
tlntsvr.exe	Telnet	C:\WINDOWS\system32\tlntsvr.exe	In Dienstverwaltung deaktivieren	Blocken	Ermöglicht den Aufruf der Kommandozeile von einem anderen Computer aus. Ist unsicher
ups.exe	Unterbrechungsfreie Stromversorgung	C:\WINDOWS\system32\ups.exe	In Dienstverwaltung deaktivieren	Blocken	Steuert eine unterbrechungsfreie Stromversorgung. Nur beim Betrieb eines Netzgeräts mit Akkusicherung nötig
vssvc.exe	Volumeschattenkopie	C:\WINDOWS\system32\vssvc.exe	Nicht beenden	Blocken	Wird von Backup-Software genutzt, die es ermöglicht, ein laufendes Windows-Betriebssystem als Image-Datei zu speichern
winlogon.exe	Windows-Logon-Prozess	C:\WINDOWS\system32\winlogon.exe	Nicht beenden	Blocken	Steuert die Anmeldung eines Benutzers am Betriebssystem Windows XP. Der Prozess gewährt dem Benutzer nur dann Zutritt, wenn Windows XP aktiviert ist. Erforderliche Basiskomponente
wmiapsrv.exe	WMI-Leistungsadapter	C:\WINDOWS\system32\wbem\wmiapsrv.exe	Nicht beenden	Blocken	Ermöglicht Managementdienste. Unter Umständen für den Betrieb einer installierten Software erforderlich
wmiprvse.exe	WMI-Dienst	C:\WINDOWS\system32\wbem\wmiprvse.exe	Nicht beenden	Blocken	Startet einen Managementdienst im Auftrag einer Software. Für jeden Managementdienst läuft eine Instanz von „wmiprvse.exe“ an; unter Umständen für den Betrieb einer installierten Software erforderlich
wpabaln.exe	Aktivierungserinnerung	C:\WINDOWS\system32\wpabaln.exe	Nicht beenden	Blocken	Wird vom Sicherheitsdienst „lsass.exe“ gestartet, selbst wenn Programmdatei im System32-Ordner fehlt
wscntfy.exe	Schnellstartverknüpfung für das Windows-Sicherheitscenter	C:\WINDOWS\system32\wscntfy.exe	Nicht beenden	Blocken	Zeigt an, dass das Sicherheitscenter aktiv ist. Dieses wird vom Service Host „svchost.exe“ gesteuert und startet das System-Tray-Icon
wuauclt.exe	Schnellstartverknüpfung für automatische Updates	C:\WINDOWS\system32\wuauclt.exe	In Dienstverwaltung deaktivieren	Blocken	Wird vom Service Host „svchost.exe“ gesteuert. Automatische Updates führen bei Konten mit eingeschränkten Benutzerrechten zu Datenverlusten. Abhilfe: Updates manuell ausführen