64-Bit-Tools für Windows 7

Download: GRMSDKX_EN_DVD.iso http://www.microsoft.com/en-us/download/details.aspx?id=8442

Windows Performance Toolkit - Leistungsmessung für Profis

http://www.computerwoche.de/software/software-infrastruktur/2490651/index8.html

http://www.winfaq.de/faq_html/Content/tip2500/onlinefaq.php?h=tip2667.htm

Mit dem kostenlosen Windows Performance Toolkit von Microsoft können Sie die Leistung eines Systems sehr effizient messen. Ausführliche Informationen erhalten Sie hier. Das Toolkit ist Bestandteil des Windows Software Development Toolkit (SDK), welches Sie kostenlos herunterladen können. Sie benötigen für den Betrieb .NET Framework 4, welches Sie über diese Seite installieren können. Haben Sie das Windows SDK mit dem Windows Performance Toolkit installiert, können Sie einen ersten Bericht zur Systemleistung erstellen:

1. Öffnen Sie dazu eine Eingabeaufforderung mit Administratorrechten.
2. Geben Sie den Befehl *xperf -start -on diageasy* ein.
3. Anschließend läuft das Tool im Hintergrund und misst die Systemleistung.
4. Starten Sie die Programme und Tools, deren Leistung Sie messen wollen. Im Hintergrund misst das Tool die Reaktionszeiten des Computers.
5. Haben Sie alle Aufgaben durchgeführt, geben Sie den Befehl *xperf -stop* ein.

Anzeigen der Messdatei nach der Messung.
Foto: Microsoft

Nach dem Stoppen der Messung erhalten Sie die Meldung, dass das Windows Performance Toolkit eine Messdatei *C:\kernel.etl* erstellt hat. Neben der Messung der Verwendung der Applikationen, können Sie mit dem Windows Performance Toolkit auch eine Messung des Bootvorgangs durchführen. Auch dazu benötigen Sie wieder eine Eingabeaufforderung mit Administratorrechten. Geben Sie dann den Befehl *xbootmgr -trace boot -resultpath c:*. Anschließend startet das Tool den Computer neu und misst den Bootvorgang. Auch hier speichert das Tool eine .etl-Datei direkt im Pfad C:\ der Festplatten.

Die erstellten Dateien können Sie mit dem *Windows Performance Analyzer* öffnen, den Sie in der Programmgruppe Windows Performance Toolkit finden. Um die Messungen anzuzeigen, öffnen Sie die Datei *C:\kernel.etl* oder die .etl-Datei des Bootvorgangs über *File/Open*.

Erhalten Sie eine Fehlermeldung beim Öffnen der Bootmessdatei, öffnen Sie diese in einer Eingabeaufforderung über den Befehl *xperfview <Pfad und Name der Datei> -tti*.

Die Anzeige der verschiedenen Bereiche blenden Sie über den Menübereich ein, den Sie durch Anklicken des linken Teils des Fensters einblenden. Klicken Sie auf die Grafik, können Sie zu Teilen der Anzeige heranzoomen, um genauere Ergebnisse zu erhalten. Dazu markieren Sie den Bereich mit der Maus, den Sie zoomen wollen, und klicken diesen mit der rechten Maustaste an. Mit dem Menübefehl *Zoom to Selection* starten Sie den Zoomvorgang. Neben Grafiken können Sie auch Tabellen anzeigen, indem Sie im Kontextmenü die Option *Summary Table* auswählen. Um eine übersichtliche Anzeige zu erhalten, entfernen Sie das Häkchen bei allen Optionen der linken Seite, die Sie nicht anzeigen wollen. Lassen Sie sich zum Beispiel beim Messen des Bootvorgangs nur *CPU Usage by Process* anzeigen, sehen Sie wie viel CPU-Last die einzelnen Prozesse verursachen. Mit *Disk I/O* sehen Sie die Festplattenzugriffe.

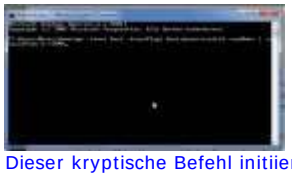
Windows 7 Performance Toolkit beschleunigt Windows-Start

http://www.pcwelt.de/ratgeber/Windows-7-Performance-Toolkit-beschleunigt-Windows-Start-5657461.html

Mit dem Windows 7 Performance Toolkit von Microsoft können Sie den Windows-Start bis ins kleinste Detail analysieren und optimieren. Der Bootvorgang eines Windows-PCs wird damit deutlich beschleunigt, Ihre Wartezeit verkürzt. Wir zeigen, wie es geht!
Bei Windows 7 hat sich Microsoft eine Menge Mühe gegeben, um den Bootvorgang zu beschleunigen. Trotz allem kommt das System mit der Zeit immer langsamer in die Gänge. Das liegt in erster Linie daran, dass auf einem frisch installierten System sehr viel weniger Programme beim PC-Start mitgeladen werden als auf einem komplett eingerichteten Windows. Was genau den Systemstart verlangsamt, lässt sich mit Bordmitteln allerdings nur schwer herausfinden. Mal sind es vom Nutzer installierte Programme, die (oft ungefragt) einzelne Komponenten oder gar das komplette Framework automatisch in den Speicher laden, mal sind es Systemdienste, die im Hintergrund gestartet werden, obwohl sie gar nicht benötigt werden.
Doch damit ist jetzt Schluss: Microsoft bietet mit dem Windows 7 Performance Toolkit ein praktisches Hilfsmittel, um die Bremser aufzuspüren. Das Programm zeichnet ein Bootprotokoll auf, in dem sämtliche Prozesse und ihr Verhalten beim PC-Start detailliert aufgeschlüsselt werden. Mit diesen Daten können Sie den Startvorgang Ihres PCs wieder auf Vordermann bringen.
Windows 7 Performance Toolkit:

Die Installation

Das Windows 7 Performance Toolkit ist Teil des Windows 7-SDKs, welches sich eigentlich an Softwareentwickler richtet. Sie haben zwei Möglichkeiten, es zu installieren.
Windows 7 Performance Toolkit (Installer und ISO)
Entweder laden Sie sich das ISO-Image des SDKs herunter, brennen es mit einem Tool wie ImgBurn auf eine DVD und installieren es manuell. Oder Sie verwenden alternativ den Web-Installer, der nur die nötigen Dateien aus dem Internet herunterlädt. Starten Sie den Installer und deaktivieren Sie im letzten Schritt vor der Installation alle Optionen außer dem Performance Toolkit in der Kategorie „Common Utilities“. Per Klick auf „Next“ startet der Download und die Installation vollautomatisch.



Dieser kryptische Befehl initiiert die Analyse des Bootvorgangs.

Systembremsen mit dem Windows 7 Performance Toolkit entlarven

Damit das Windows 7 Performance Toolkit die Bootperformance analysieren kann, müssen Sie zunächst ein entsprechendes Protokoll erstellen. Das funktioniert über das Kommandozeilentool xbootmgr. Geben Sie im Startmenü „cmd“ ein, klicken Sie das Ergebnis mit der rechten Maustaste an und wählen Sie „Als Administrator ausführen. Tippen Sie nun folgenden Befehl in die Kommandozeile ein:
xbootmgr -trace boot -traceFlags base+power+cswitch -numRuns 1 -resultPath C:\TEMP
Nach einer Rückmeldung startet Windows 7 neu und erstellt dabei ein ausführliches Protokoll des Bootvorgangs. Warten Sie nach dem Hochfahren unbedingt, bis das Meldungsfenster des Performance Toolkits verschwindet, damit die Messwerte nicht verfälscht werden. Navigieren Sie nun zum Ordner „C:\Temp“ (diesen können Sie natürlich ändern, indem Sie den Kommandozeilenbefehl anpassen). Hier finden Sie eine Datei namens „boot_BASE+CSWITCH+POWER_1.etl“, die Sie per Doppelklick mit dem Windows Performance Analyzer öffnen können. Dieses zeigt Ihnen anhand einer Zeitliste detailliert, was beim Windows-Start auf Ihrem PC passiert.

Die Aufzeichnung des Bootprotokolls dauert länger als der normale Windows-Start; warten Sie aber in jedem Fall, bis die Dialogbox verschwindet.

Über das Menü auf der linken Seite können Sie die relevanten Informationen einblenden, wobei besonders die Daten interessant sind, die die Prozesse behandeln. „CPU Usage by process“ zeigt beispielsweise, welche Programme den Prozessor während des Startvorgangs auslasten. Fällt eine

der Linien besonders ins Auge, fahren Sie mit der Maus über den Graphen, um den damit verbundenen Prozess zu identifizieren; alternativ können Sie über das Menü auf der rechten Seite genau festlegen, welche Prozesse das Programm anzeigt.

Windows-Systemdienste sind häufig der Grund für einen lahmen Start. Hier verzögert der Hintergrunddienst des Tools GesWall den Bootvorgang.

Neben der CPU ist auch die Festplattenauslastung ein Indiz für Systembremsen. Informationen darüber erhalten Sie unter dem Punkt „Disk Utilization by Process“; auch hier sollten Sie wieder auf größere Ausschläge der Graphen achten. Zu guter Letzt lohnt sich noch ein Blick in den Bereich „Services“. Hier sehen Sie, welche Systemdienste Windows beim Hochfahren startet. Sollten Ihnen hier besonders lange Bootzeiten auffallen, sollten Sie prüfen, ob eine Deaktivierung in Frage kommt.

Autoruns ergänzt das Windows 7 Performance Toolkit

Mit Autoruns aus der Sysinternals Suite schalten Sie die lähmenden Autostarts ab, ohne die Programme gleich deinstallieren zu müssen.

Haben Sie die Bremsklötze erst einmal identifiziert, hilft ein weiteres Microsoft-Tool bei der Deaktivierung. Die Rede ist von Autoruns aus der Systinternals-Suite, das Sie kostenlos herunterladen können . Das Programm listet sämtliche Dienste, Programme und Treiber auf, die Windows beim Start lädt, und lässt Sie diese über ein einfaches Häkchen abschalten. Suchen Sie einfach die entsprechenden Einträge im Reiter „Everything“ beziehungsweise in den Unter-Kategorien „Logon“ und „Services“. Bei der Entscheidung, ob Sie einen bremsenden Windows-Dienst oder lähmende Autostarts wirklich problemlos deaktivieren können, hilft im Zweifel eine Google-Suche. Praktischerweise führen Sie diese direkt über Autoruns aus, indem Sie den entsprechenden Eintrag mit der rechten Maustaste anklicken und „Search Online“ auswählen. Im Zweifel sollten Sie lieber die Finger von den Einträgen lassen; sollte es dennoch einmal zu Problemen beim Booten kommen, können Sie diese durch eine Rückkehr zum alten Wiederherstellungspunkt beheben.

Auch Treiber können den Windows-Start ausbremsen. Fast 64 Sekunden lang blockiert das Laden des Norton Internet Security-Treibers hier den Systemstart.

Detailanalyse mit dem Performance Toolkit

Wenn Sie durch die Deaktivierung von Autostarts und diversen Windows-Diensten noch nicht den nötigen Schub beim Windows-Start erhalten, können Sie mit dem Performance Toolkit auch mögliche Treiberkonflikte aufspüren. Erweitern Sie den Kommandozeilenbefehl dazu um den Zusatz „+DRIVERS“. Dadurch wird beim Start auch das Laden der Gerätetreiber protokolliert, sodass Sie im Performance Analyzer unter „Driver Delay“ sehen können, ob ein Treiber für Verzögerungen sorgt. Ist dies der Fall, sollten Sie nach einem Update suchen oder den fehlerhaften Treiber gegebenenfalls deinstallieren. Auch den Wechsel und das Wiederaufwachen aus dem Standby- beziehungsweise Ruhemodus lässt sich mit dem Tool analysieren; ersetzen Sie dazu einfach den Parameter „-trace boot“ mit „-trace standby“ oder „-trace hibernate“ und wecken Sie den PC erneut.

http://www.pcwelt.de/ratgeber/Profi-Analyse-Windows-Performance-Toolkit-4380433.html

Das Windows Performance Toolkit (WPT) ist ein Teil der Programmsammlung Microsoft Windows SDK.

So protokollieren Sie das Starten und Beenden

Als Vorbereitung schließen Sie alle geöffneten Dateien, denn das Windows Performance Toolkit (WPT) wird gleich den PC neu starten. Da Sie das WPT über die Eingabeaufforderung von Windows steuern, starten Sie diese über die Windows-Taste, die Sie zusammen mit der Taste R drücken. Geben Sie in das folgende Fenster den Befehl cmd ein, und klicken Sie auf „OK“. Es öffnet sich dann die Windows-Eingabeaufforderung. Um den Startvorgang von Windows zu protokollieren, geben Sie in die Eingabeaufforderung diesen Befehl ein, gefolgt von der Taste Enter:

xbootmgr -trace boot –resultpath C:

Unter Windows Vista fragt die Benutzerkontensteuerung nach Administratorrechten für die Aktion, was Sie mit „Fortsetzen“ gewähren. Unter Windows 7 ist das nicht nötig. Es erscheint unter beiden Windows-Versionen die Information, dass Windows in Kürze neu startet, was danach automatisch geschieht. Nach dem Neustart erscheint ein Infofenster, dass WPT noch zwei Minuten wartet, bis alle Programme geladen sind. Lassen Sie die Zeit verstreichen, und bedienen Sie Tastatur und Maus erst wieder, wenn die Info verschwunden ist.

Wollen Sie das Herunterfahren des Systems analysieren, dann geben Sie diesen Befehl ein, gefolgt von der Taste Enter:

xbootmgr -trace shutdown –resultpath C:

Auch hier startet das Windows Performance Toolkit den PC neu. Das Ergebnis der Untersuchung landet in beiden Fällen direkt auf dem Laufwerk C: in einer Datei namens Boot_base+cswitch_1.etl für den Startvorgang und in einer Datei namens Shutdown_base+cswitch_1.etl fürs Beenden.

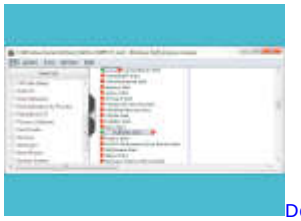
So erkennen Sie die Bremsklötze auf Anhieb

Mit dem Befehl Xbootmgr.exe aus dem Windows Performance Toolkit haben Sie bereits ein Protokoll über die Systemvorgänge Ihrer Windows-Installation erstellt. Die Protokolldatei mit der Endung .etl ist bereits mit dem Programm Windows Performance Analyzer (WPA) verknüpft. Öffnen Sie das Protokoll für den Windows-Start mit einem Doppelklick auf die Datei Boot_base+cswitch_1.etl, und bestätigen Sie unter Windows 7 noch ein Infofenster.

Der WPA zeigt Ihnen per Grafik eine ganze Menge Information. Sie finden die Bremsklötze beim Systemstart am schnellsten, wenn Sie überflüssige Grafiken deaktivieren. Klicken Sie dafür auf den Pfeil am linken Rand. Es öffnet sich eine Liste („Frame List“) mit allen verfügbaren Werten. Entfernen Sie die Haken vor allen Zeilen bis auf den vor „Services“. Lassen Sie die Liste nun wieder über einen Klick auf den Pfeil verschwinden.

Es bleibt die Grafik zu „Services“, die überwiegend aus roten Quadraten plus Namen besteht. Die X-Achse unten zeigt die verstrichene Startzeit an. Meist ist die Grafik oben abgeschnitten. Sie bekommen die Liste komplett angezeigt, wenn Sie mit der linken Maustaste den unteren Rand der Grafik packen und nach unten ziehen. Das geht nur, wenn sich das Programmfenster nicht im Vollbildmodus befindet. Unter Umständen müssen Sie den Vorgang wiederholen. Sie sollten zudem die Grafik etwas vergrößern, indem Sie die Taste Strg gedrückt halten und dann das Mausrad nach vorne drehen. So bekommen Sie einen bessere Detailansicht.¨

Bremsklötze hinterlassen Bremsspuren: Programme und Dienste, die blitzschnell starten, tauchen in der Grafik als rotes Quadrat auf. Ansonsten markiert Rot das Ende des Ladevorgangs, Grün den Startzeitpunkt. Er liegt bei flotten Programmen fast direkt unter dem roten Quadrat. Bremsklötze sind dagegen als lange Balken dargestellt. In der Abbildung fällt etwa sofort der Balken mit dem Namen „RUBotSrv“ auf.


Der Windows Performance Analyzer zeigt Ihnen sehr anschaulich, welches Programm den Windows-Start bremst. Hier ist es etwa die Software RUBotSrv.

Wenn Ihnen der Name eines Balkens nicht direkt verrät, zu welchem Programm er gehört, können Sie in die Tabellenansicht wechseln und dort den Programm- oder Dienstenamen ablesen. Klicken Sie zu diesem Zweck mit der rechten Maustaste auf die Grafik und wählen Sie im aufklappenden Menü „Summary Table“. In der Tabelle sehen Sie sämtliche Werte, wenn Sie in der Spalte „Group“ auf alle Kästchen mit Kreuz klicken. Nun finden Sie in der Spalte „Service“ den Namen aus der Grafik und in der Spalte „Container“ den Namen des Programms oder des Dienstes. Im Beispiel mit „RUBotSrv“ ist es recht banal Rubotsrv.exe. Nach diesem Namen können Sie nun im Internet suchen.

Das Herunterfahren analysieren: Die Bremsklötze beim Beenden von Windows finden Sie in der Datei Shutdown_base+cswitch_1.etl. Deaktivieren Sie in der „Frame List“ alle Einträge bis auf „Process Lifetimes“ und „Services“. Die Balken sind hier generell viel länger. Das ist Okay. Nehmen Sie sich die längsten vor, und suchen Sie wie zuvor beschrieben den zugehörigen Programmnamen in der Tabelle.

Suche im Internet: Bremsklötze identifizieren

Sie haben über die Methoden zuvor einzelne Programmnamen als Bremsklötze identifiziert. Nun finden Sie über eine Suche im

Internet heraus, welche Software dahinter steckt und ob diese vielleicht schon als Bremsklotz bekannt ist. Ob sich das Programm reparieren lässt, ob Sie ganz darauf verzichten können oder ob Sie mit dem Bremsklotz leben müssen, entscheiden Sie für jeden Einzelfall neu.

In den beiden Beispielen oben entpuppten sich die Dateien Avguard.exe und Rubotsrv.exe als problematisch. Im Falle von Avguard.exe ergibt eine einfache Suche nach diesem Dateinamen via Google, dass es sich um einen Bestandteil des Antiviren-Programms Antivir vom Hersteller Avira handelt. Natürlich sollten Sie nicht auf den Schutz verzichten, den das Antiviren-Programm bietet. Doch es ist gut möglich, dass eine fehlerhafte Installation des Programms an der Verzögerung schuld ist.

Eine De-Installation über „Windows-Logo ➞ Systemsteuerung ➞ Programm deinstallieren“ und eine erneute Installation kann helfen. Das Programm Rubotsrv.exe gehört ebenfalls zu einer Sicherheits-Software. Es soll Rootkits, also Virenmit Tarnkappe, aufspüren. Das Programm wurde auf dem PC vor einigen Monaten nur testweise installiert und dann vergessen. Es kann bedenkenlos über die Systemsteuerung beseitigt werden.

Spezialsuche für Programme: Wenn Ihnen Google keine hilfreichen Treffer ausgibt, versuchen Sie es über spezielle Internetseiten. Für Programme empfiehlt sich die Datenbank unter file.net. Handelt es sich nicht um ein Programm, sondern um eine DLL-Datei, versuchen Sie es über liutilities.

Vorsicht bei Virennamen: Viele Viren tarnen sich, indem sie die Namen von harmlosen Windows-Programmen annehmen. Bei Ihrer Suche bei Google könnten Sie deshalb auch Treffer in Diskussionsforen angezeigt bekommen, in denen PC-Nutzer über solche Viren klagen. Das heißt aber noch lange nicht, dass es sich bei Ihrer Datei ebenfalls um diesen Virus handelt. Hier gilt es, nicht nur den Programmnamen, sondern auch den genauen Speicherort zu vergleichen. Besteht weiterhin ein Virenverdacht, dann überprüfen Sie die Datei auf virustotal.com.

AutoRuns

http://www.pcwelt.de/downloads/AutoRuns-580539.html

Mit diesem kostenlosen Tool wird Ihr Windows-Start auf Schnelligkeit getrimmt: Autoruns zeigt Ihnen übersichtlich die gestarteten Routinen an und lässt Sie diese gezielt abstellen. AutoRuns 11.34 ist ein Alternative zum Windows-internen Autostart-Konfigurationsmenü. Wenn Windows startet, starten gleichzeitig etliche Programme und Routinen mit. Das verlangsamt nicht nur das Hochfahren, sondern belegt auch unnötig viele Systemressourcen. Mit dem englischsprachigen Microsoft-Tool AutoRuns starten Sie nur das, was Sie wirklich brauchen. Dazu zeigt das Gratis Tool AutoRuns – geordnet in Registerkarten – verschiedene Bereiche und Speicherorte und die dort geöffneten Routinen. Mit Hilfe des Häkchens entscheiden Sie, welche Anwendung beim nächsten Start der Freeware AutoRuns geöffnet werden soll.

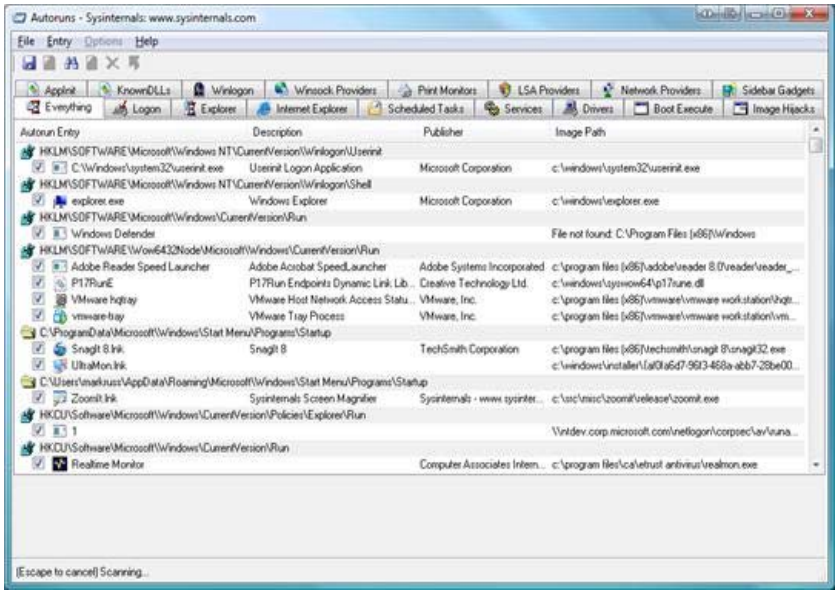
Ein weiterer Vorteil: AutoRuns muss nicht installiert werden.

http://technet.microsoft.com/de-de/sysinternals/bb963902.aspx

Dieses Dienstprogramm ist im Vergleich zu allen anderen Startüberwachungsprogrammen mit den derzeit umfassendsten Informationen zu den Autostartpfaden ausgestattet. AutoRuns zeigt, welche Programme für die Ausführung beim Starten des Systems oder bei der Benutzeranmeldung konfiguriert sind, wobei die Einträge in der Reihenfolge aufgeführt sind, in der sie in Windows verarbeitet werden. Zu diesen Programmen gehören die Anwendungen im Startordner sowie in den Registrierungsschlüsseln „Run“, „RunOnce“ und anderen Schlüsseln. Sie können *AutoRuns* so konfigurieren, dass auch andere Pfade berücksichtigt werden, beispielsweise Explorer-Shellerweiterungen, Symbolleisten, Browserhilfsobjekte, Winlogon-Benachrichtigungen, Autostartdienste und vieles mehr. *AutoRuns* geht weit über die Möglichkeiten des Dienstprogramms MSConfig in Windows ME und Windows XP hinaus.

Mit der Option **Hide Signed Microsoft Entries** in *AutoRuns* können Sie sich auf Autostartabbilder von Drittanbietern konzentrieren, die in Ihr System integriert wurden. Darüber hinaus ist es auch möglich, die Autostartabbilder für andere auf dem System konfigurierte Benutzer zu betrachten. Das Downloadpaket enthält außerdem das Befehlszeilenprogramm Autorunsc, mit der die Daten im CSV-Format ausgegeben werden können.

Sie werden sich wundern, wie viele ausführbare Dateien automatisch gestartet werden!



Verwendung

Führen Sie einfach *AutoRuns* aus, und schon sehen Sie die derzeit konfigurierten Autostartanwendungen und dazu eine vollständige Liste aller Registrierungs- und Dateisystempfade, die für die Autostartkonfiguration zur Verfügung stehen. Mit AutoRuns werden die folgenden Autostartpfade angezeigt: Anmeldeeinträge, Explorer-Add-Ons, Internet Explorer-Add-Ons (z. B. Browserhilfsobjekte), Appinit-DLLs, Abbildhijacks, Abbilder für die Ausführung beim Systemstart, Winlogon-Benachrichtigungs-DLLs, Windows-Dienste und Winsock-Mehrschicht-Dienstanbieter. Die automatisch gestarteten Objekte sind auf den einzelnen Registerkarten in Kategorien gegliedert.

Um die Eigenschaften einer ausführbaren Datei abzurufen, die für die automatische Ausführung konfiguriert ist, markieren Sie diese Datei, und wählen Sie im Menü die Option **Properties**, oder klicken Sie auf die entsprechende Schaltfläche in der Symbolleiste. Wenn Process Explorer ausgeführt wird und ein Prozess aktiv ist, mit dem die ausgewählte ausführbare Datei ausgeführt wird, dann gelangen Sie mit der Option **Process Explorer** im Menü **Entry** zum Dialogfeld mit den Eigenschaften für den Prozess, der das ausgewählte Abbild ausführt.

Um zum angezeigten Registrierungs- oder Dateisystempfad oder auch zur Konfiguration eines Autostartelements zu navigieren, markieren Sie das gewünschte Element, und wählen Sie dann die Menüoption **Jump**, oder klicken Sie auf die entsprechende Schaltfläche in der Symbolleiste.

Soll ein Autostarteintrag deaktiviert werden, deaktivieren Sie das zugehörige Kontrollkästchen. Zum Löschen eines Autostart-Konfigurationseintrags wählen Sie die Menüoption **Delete**, oder klicken Sie auf die entsprechende Schaltfläche in der Symbolleiste.

Um Autostartabbilder für verschiedene Benutzerkonten abzurufen, wählen Sie im Menü **User** die entsprechenden Einträge aus.

Weitere Informationen zu den Anzeigeoptionen und andere Angaben finden Sie in der Onlinehilfe.

Verwendung von Autorunsc

Autorunsc ist die Befehlszeilenversion von AutoRuns. Hier gilt die folgende Syntax:

Verwendung: autorunsc [-a] | [-c] [-b] [-d] [-e] [-h] [-i] [-l] [-m] [-n] [-p] [-r][-s] [-v] [-w] [Benutzer]

-a	Alle Einträge anzeigen.
-b	Ausführung beim Systemstart.
-c	Druckausgabe als CSV.
-d	Appinit-DLLs.
-e	Explorer-Add-Ons.
-g	Sidebar gadgets (Vista and higher).
-h	Abbildhijacks.
-i	Internet Explorer-Add-Ons.
-l	Anmeldestarts (Standardeinstellung).
-m	Signierte Microsoft-Einträge ausblenden.
-n	Winsock-Protokollanbieter.
-p	Druckermonitortreiber.
-r	LSA-Anbieter.
-s	Autostartdienste und nicht deaktivierte Treiber.
-t	Geplante Aufgaben.
-v	Digitale Signaturen überprüfen.
-w	Winlogon-Einträge.
user	AutoRuns für das angegebene Benutzerkonto sichern.