

Übung 2: Dienste, Umgebungsvariablen und der Bootvorgang unter Windows

2.1 Wichtige Dienste unter Windows

Ziel der Übung:

In den folgenden – kurzen – Übungen werden Sie überblicksweise den *Process Explorer* kennenlernen sowie in der Systemsteuerung eine Umgebungsvariable anlegen.¹

Wir verwenden in dieser Übung Windows 7 als Beispiel-Betriebssystem.

Process Explorer:

Der Process Explorer liefert ähnliche Informationen wie der Task Manager, jedoch bietet er erweiterte Diagnose- und Analysemöglichkeiten. Desweiteren ist die Darstellung der Prozesse optisch gut aufbereitet².

(Hinweis: Ein Prozess ist im Sinne des Betriebssystems eine Ablaufumgebung für Programme mit zugeordnetem Speicher.)

Übung:

1. Laden Sie den Process Explorer herunter (entweder über die Microsoft TechNet-Seite oder einfach danach suchen ☺)
2. Entpacken Sie das Programm in Ihr Home-Laufwerk und starten Sie die Datei procexp.exe
3. Welche PID hat der Leerlaufprozess?
4. Suchen Sie den Prozess svchost.exe. Wozu dient er?
5. Starten Sie einen neuen Prozess (bspw. eine Kommandozeile öffnen – Start → Ausführen → cmd eintippen).
6. Suchen Sie den neu gestarteten Prozess im Process Explorer und betrachten Sie die Informationen zum Prozess!

¹ Ein möglicher Suchbegriff für Google wäre „Umgebungsvariable“

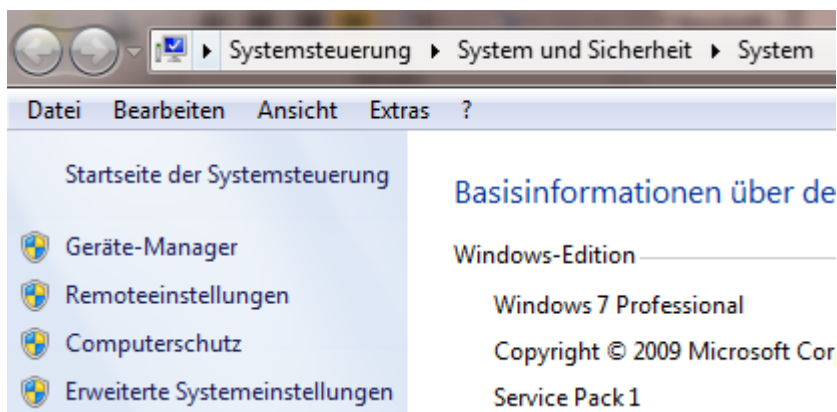
² Weitere Informationen unter <http://technet.microsoft.com/de-de/sysinternals/bb896653> [letzter Zugriff am 15.03.2014]

2.2 Anlegen einer Umgebungsvariablen unter Windows

Systemsteuerung:

Wechseln Sie in der Systemsteuerung zum Punkt *System*, welcher sich unter *System und Sicherheit* befindet (Alternative: Tastenkombination *Windows-Taste + Pause*).

Rufen Sie anschließend *Erweiterte Systemeinstellungen* auf und klicken Sie dann auf *Umgebungsvariablen*. Hier können Sie Benutzer- und Systemvariablen anlegen³.

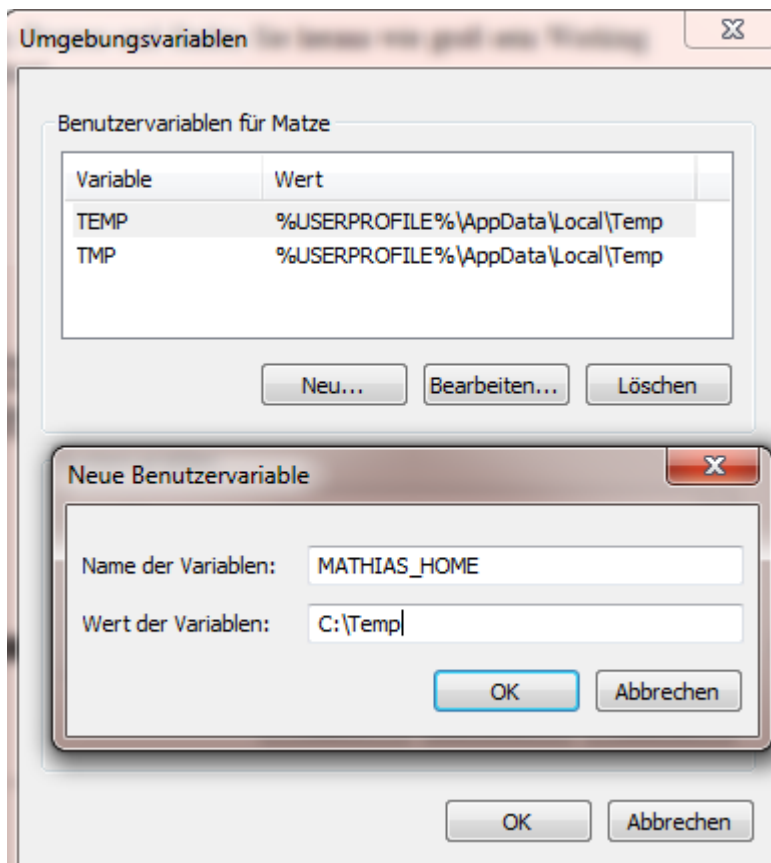


Definieren einer Umgebungsvariable (hier: Benutzervariable):

Bevor Sie eine Umgebungsvariable festlegen, öffnen Sie ein Kommandozeile (Start → *cmd* eingeben bzw. Tastenkombination *Windows-Taste + R* → *cmd* eingeben). Die Microsoft-Kommandozeile wird nun angezeigt. Mit dem Befehl *set* können Sie den Wert einer Umgebungsvariablen anzeigen. Geben Sie nun *set IHRVORNAME_HOME* ein. Den Namensteil *IHRVORNAME* ersetzen Sie bitte durch Ihren Vornamen. Der Befehlsaufruf müsste nun eine Fehlermeldung bringen. Wechseln Sie nun erneut, wie oben beschrieben, in den Dialog *Umgebungsvariablen*.

Es erscheint ein Fenster, in dem sämtliche Umgebungsvariablen angezeigt werden. Klicken Sie im oberen Abschnitt (*Benutzervariablen*) auf *Neu* und geben Sie als Name der Variablen *IHRVORNAME_HOME* und als Wert der Variablen *C:\TEMP* ein (siehe nachfolgende Abbildung). Aktivieren Sie nun wieder das Kommandozeilenfenster und geben Sie erneut *set IHRVORNAME_HOME* ein. Der Aufruf müsste nun erneut eine Fehlermeldung provozieren. Schließen Sie das Kommandozeilenfenster und starten Sie es erneut. Geben Sie nochmals *set IHRVORNAME_HOME* ein. Mit welchem Ergebnis?

³ Aufgrund eingeschränkter Rechte können Sie an dieser Stelle nur Benutzervariablen anlegen.



2.3 Bootvorgang bei Windows

Ziel der Übung:

Kennenlernen des Bootvorgangs unter Windows.

Ablauf:

Windows Bootvorgang	
POST (Power On Self Test)	Analog zu Bootvorgang Linux aus Übung 3
Bootloader	Analog zu Bootvorgang Linux aus Übung 3
Initialisieren des Kernels	Laden des Kernels NTOSKRNL.EXE (z.B. unter c:\WINDOWS\system32\) <ul style="list-style-type: none"> • Initialisiert die niedrigen Gerätetreiber (low level driver), die in der vorherigen Phase geladen wurden. • Laden und Initialisieren der anderen Gerätetreiber. • Startet Programme wie chkdsk. • Laden und Initialisieren der Services (Dienste) un-

	<p>ter Windows</p> <ul style="list-style-type: none">• Erstellen der Auslagerungsdatei (Pagefile).• Starten der Subsysteme, die Windows benötigt. <p>Laden des Session-Managers SMSS.EXE, der für die Ausführung vieler paralleler Prozesse zuständig ist. Der Session-Manager entnimmt der Registry die Programme, welche beim Systemstart auszuführen sind.</p> <p>Weiterhin, wird autochk.exe zur Kontrolle der Partitionen geladen, um dann anschließend den VMM (Virtual Memory Manager) zu starten. Danach werden die Subsysteme und die Dienste, die im Dienstmanager definiert wurden, gestartet.</p>
--	--

Übung: Versuchen Sie herauszufinden, welche Funktionalität sich hinter den folgenden Prozessen verbirgt. (Hinweis: Der *Process-Explorer* gibt hier hilfreiche Hinweise.)

- lsass.exe
- csrss.exe
- svchost.exe
- smss.exe

Je nach Windows-Version sieht der Taskmanager unterschiedlich aus (hier z.B. Windows 7):

