Alles zu "svchost.exe"

Im Task-Manager von Windows taucht gleich mehrfach die Datei "svchost.exe" auf. Was hinter dieser Datei steckt, erklärt dieser Artikel.

Im Task-Manager von Windows ist auf der Registerkarte "Prozesse" mehrmals der Eintrag "svchost.exe" zu sehen. Es handelt sich dabei um eine Systemdatei von Windows XP, Vista und 7. Was die "svchost.exe" genau ist und macht, zeigt der Artikel.

Windows-Dienste

Die Datei "svchost.exe" liegt im Verzeichnis "C:\Windows\System32". Windows führt damit eigene Dienste wie die Windows-Firewall aus. Weitere Dienste sind etwa dafür zuständig, USB-Geräte zu erkennen oder den Drucker anzusteuern. Auch Netzwerkverbindungen werden von Diensten gesteuert. Ausserdem ist die Datei "svchost.exe" für die wichtige Funktion Windows Update zuständig.

Technisch gesehen ist "svchost.exe" ein Host-Prozess, der Dienste mit Hilfe von DLL-Dateien ausführt. DLL steht für Dynamic Link Library. Vereinfacht ausgedrückt führt die Datei "svchost.exe" Dienste aus, indem sie für jeden Dienst den Programmcode in der zugehörigen DLL-Datei abarbeitet.

Jede Instanz der Datei "svchost.exe" startet eine andere Gruppe von Windows-Diensten. Wie viele Instanzen der "svchost.exe" laufen, hängt davon ab, welche Windows-Dienste im Hintergrund gerade aktiv sind. Welche Dienste eine gemeinsame Instanz der Datei "svchost.exe" nutzen, zeigt die Registry im Schlüssel "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\svchost".

Tasklist

Das Kommandozeilen-Tool Tasklist listet besser als der Task-Manager alle "svchost.exe"-Instanzen samt Windows-Diensten.

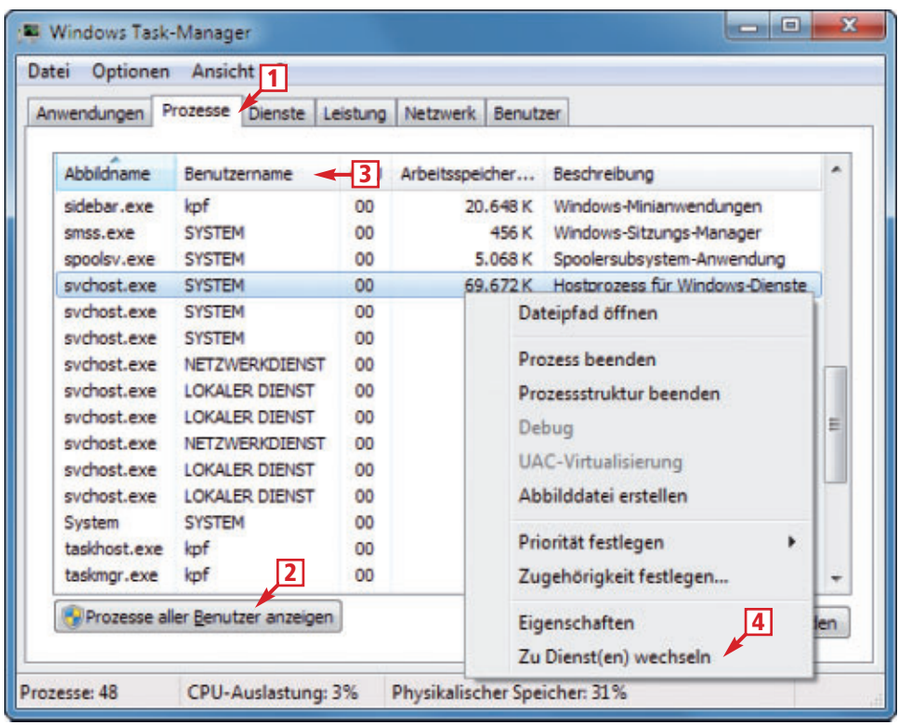
Tasklist ist in Windows XP Professional, Vista und Windows 7 enthalten. Starten Sie die Eingabeaufforderung mit [Windows R] und `cmd`. Geben Sie danach `tasklist /svc` ein.

Unter "Abbildname" steht jede Instanz der Datei "svchost.exe", dahinter in der Spalte "Dienste" stehen die Windows-Dienste.

Tasklist gibt die Kurznamen der Dienste an. Was sie bedeuten, steht unter http://social.technet.microsoft.com/wiki/contents/articles/windows-7-default-services.aspx.

So geht's: Windows Task-Manager

Der Task-Manager in Windows Vista und 7 zeigt, welche Dienste sich hinter einer Instanz von "svchost.exe" verbergen. Den Task-Manager starten Sie mit [Windows Umschalt Esc].



1 Prozesse
Das Register zeigt eine Übersicht aller laufenden Prozesse.

2 Prozesse aller Benutzer anzeigen
Zeigt sämtliche Prozesse, also auch Prozesse, die Windows selbst ausführt, wie "svchost.exe".

3 Benutzername
Der Benutzername, der "svchost.exe" gestartet hat, ist ein erster Anhaltspunkt, welcher Dienst dahintersteckt.

4 Zu Dienste(en) wechseln
Zeigt, welche Dienste zu einer Instanz von "svchost.exe" gehören.

Windows Task-Manager

Einen Überblick über die Datei "svchost.exe" und die laufenden Dienste erhalten Sie im Task-Manager von Windows.

Starten Sie ihn mit [Strg Umschalt Esc]. Wechseln Sie zum Register "Prozesse". Es zeigt alle laufenden Prozesse.

Windows Vista und 7: Windows Vista und 7 zeigen nur die laufenden Prozesse an, die von Ihrem Benutzerkonto gestartet wurden. Da "svchost.exe" vom Windows-System selbst gestartet wird, müssen Sie die Datei erst sichtbar machen. Klicken Sie dazu im Windows Task-Manager auf die Schaltfläche "Prozesse aller Benutzer anzeigen".

Der Task-Manager informiert darüber, welche Windows-Dienste sich hinter einer Instanz der "svchost.exe" verbergen. Die Spalte "Benutzername" gibt einen ersten Hinweis: Der Benutzername "SYSTEM" steht für einen Systemdienst wie beispielsweise Windows Update. Der Benutzer "NETZWERKDIENST" steht für Dienste im Zusammenhang mit Netzwerken. Der Benutzername "LOKALER

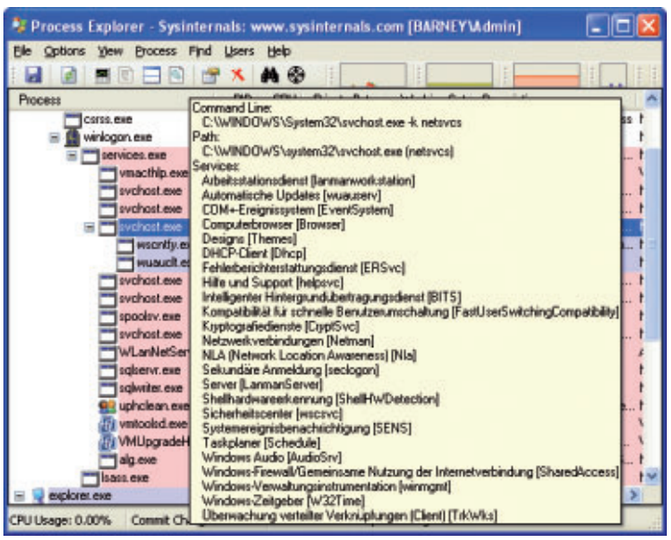
DIENST“ steht für andere Dienste wie das Sicherheitscenter.

Um zu sehen, welche Dienste sich hinter einer Instanz von “svchost.exe“ verbergen, klicken Sie zunächst mit der rechten Maustaste auf eine Instanz und wählen dann “Zu Dienst(en) wechseln“.

Weitere Details zum Windows Task-Manager stehen im Kasten “So geht's: Windows Task-Manager“ auf der Seite 26.

Windows XP: Der Task-Manager von XP zeigt die Dienste der Datei “svchost.exe“ nicht an. Nutzen Sie stattdessen das Tool Process Explorer 15.04 (kostenlos, http://technet.microsoft.com/de-de/sysinternals/bb896653 und auf).

Bewegen Sie in der Prozessliste des Process Explorer den Mauszeiger über eine Instanz der “svchost.exe“.



Process Explorer 15.04: Das Tool zeigt unter XP alle Dienste einer Instanz der Datei “svchost.exe“ an (Bild A)

Auf DVD

Das Tool Process Explorer 15.04 finden Sie auf in der Rubrik “Computer, svchost.exe“.

Ein Tooltipp zeigt alle dahinterstehenden Dienste an (Bild A).

Finger weg von den Diensten

Gelegentlich lastet eine Instanz der “svchost.exe“ den PC im Leerlauf voll aus: Wie im Windows Task-Manager in der Spalte “CPU-Auslastung“ zu sehen, steigt die Prozessorauslastung stark an. Ursache ist ein Dienst wie Windows Update, der Aktualisierungen installiert. Die einzelnen Instanzen verbrauchen zudem viel Arbeitsspeicher – bis zu 100 MByte.

Dennoch sollten Sie die Konfiguration der Dienste – sie lässt sich mit [Windows R] und `services.msc` aufrufen – nicht ändern: Selbst für erfahrene Nutzer ist es schwer zu entscheiden, welcher Dienst ein wichtiger Bestandteil von Windows ist. Zudem sind aktuelle Computer so schnell, dass es kaum eine Rolle spielt, welcher Dienst gerade läuft.

Übrigens: Manche Schädlinge tarnen sich mit ähnlichen Dateinamen wie “scvhost.exe“ oder “svhost.exe“. Oder sie stecken in einem anderen Ordner als das Windows-Original. Ein regelmässiger Blick in den Task-Manager von Windows und ein Virenscanner mit den aktuellen Virendefinitionen sind daher Pflicht. ■

Konstantin Pfliegl/jb

G DATA INTERNETSECURITY HOMESERVER ADVERTORIAL

Optimaler Schutz für Heimnetzwerke: G Data InternetSecurity für HomeServer

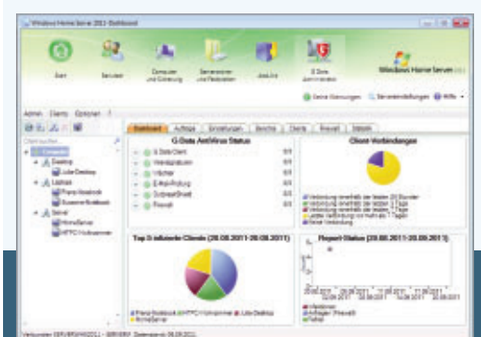
Mit G Data InternetSecurity für HomeServer bringt der IT-Security-Hersteller eine einzigartige Sicherheitslösung für das heimische Netzwerk in den Handel. Sie schützt Heimnetzwerke von bis zu 5 PCs.

Heimnetzwerke, die auf gemeinsame Ressourcen, wie Internetzugang, Drucker oder Video- und Bilddaten zurückgreifen, werden bei Anwendern immer beliebter. Nicht selten verfügen Schweizer Haushalte bereits über drei oder mehr Computer. Für diese Anwender bringt der deutsche Sicherheitsspezialist G Data jetzt eine Sicherheitslösung auf den Markt. Mit G Data InternetSecurity für HomeServer können Home-Admins dank der zentralen Managementkonsole alle Sicherheitseinstellungen, wie Virenschutz oder Firewall-Regeln, bequem von einem PC aus für alle Einzelgeräte vornehmen. G Data InternetSecurity für HomeServer schützt bis zu 5 PCs und ist zum Preis von 129 Franken ab Dezember im Handel erhältlich.

Die Installation von Microsoft Homeserver 11 ist dabei nicht zwingend erforderlich – denn: G Data InternetSecurity für HomeServer ist auf jedem System mit Windows XP, Vista oder Windows 7 im vollen Funktionsumfang einsetzbar.

Entsprechend der Lizenzgrösse erhalten Käufer von G Data InternetSecurity für Homeserver fünf kostenfreie Lizenzen von G Data MobileSecurity für Android zur Absicherung ihrer Smartphones und Tablet-PCs. So sind auch mobile Geräte jederzeit wirkungsvoll vor Angriffen geschützt.

Weitere Infos: www.gdata.ch



Zentrale Managementkonsole: Über das Dashboard und die intuitive Benutzeroberfläche haben Home-Admins den Sicherheitsstatus der heimischen Rechner immer im Blick.