3.32 Windows XP Systemkern wird geladen

Der Systemstart

Wie bereits im Thema 3.31 beschrieben wurde, beginnt der Ladeprozess des Systemkerns mit dem Herzstück des Betriebssystems *ntoskrnl.exe.* Danach wird der Kern des Betriebssystems im „rasanten“ Tempo in modularen Ebenen auf Grundlage des NTFS-Dateisystems Schicht für Schicht aufgebaut. Um die Wechselwirkung der Bestandteile zu verstehen, soll kurz auf die verschiedenen Ebenen (Layer) eingegangen werden. Der Systemkern (Kernel) ist als Exekutive zwischen Hardware und Anwendungen - Benutzerebene gelegt. Man spricht hier auch von einer Ringstruktur.

Zunächst werden die Treiber für den Kernelmodus geladen. Das beginnt mit einem Paket bestehend aus *ntoskrnl.exe, hal.dll, kdcom.dll, bootvid.dll,* das die Hardware des Computers erfasst und mit dem *hardware abstractions layer (hal)* die unterste Schicht des Systemkerns darstellt. Somit ist der direkte Zugriff von Programmen auf die Hardware verhindert.

Der Ladeprozess erfolgt danach schrittweise in einer Rangfolge, die im Registryschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services - REG_DWORD - Wert / Start festgelegt ist. Treiber mit Wert=0 werden während der Kernel-Ladephase, weitere Treiber mit Wert=1 in der Ladephase der Dienste geladen. Treiber mit Wert=3 werden aktiviert aber nicht initialisiert und diejenigen mit Wert=4 nicht aktiviert. Die Treiber initialisieren die erforderlichen Prozesse und Gerätetreiber für Festplatten, Plug- und Play-Systeme, GUI (Grafische Benutzerschnittstelle), Sicherheits- und Systemschutzprozesse und Netzwerkschnittstellen. Der Umfang der geladenen Treiber kann im *Abgesicherten Modus* durch Startprotokollierung gespeichert und in der Datei *windows\ntbtlog.txt* nachkontrolliert werden. Dazu ist zu bemerken, dass mit der Verbesserung der Systemsicherheit durch Service Packs von Service Pack zu Service Pack der Umfang der Treiber vergrößert wurde. So ist mit Installation des Service Pack 3 die Zahl der im Start geladenen Treiber auf das Dreifache angewachsen.

Im Prozess des Ladens des Systemkerns werden Prozess-Subsysteme installiert, die als Windows - Exekutive im Kernelmodus wirken. Folgende Exe-Dateien sind für die Arbeit des Betriebsystems wichtig. Sie werden in der Registerkarte *Prozesse* des Task-Managers (Thema 3.33) angezeigt.

Dazu gehören folgende Prozesse:

smss / smss.exe der Sitzungsmanager, als erstes Subsystem, über das die weiteren Subsysteme und Dienste gestartet werden.
explorer / explorer.exe ist unverzichtbar und für die Dateinavigation zuständig. Dazu gehört unter anderem der Windows Explorer und die Taskleiste.
lsass / lsass.exe, (**L**ocal **S**ecurity **A**uthority **S**ub**s**ystem), der lokale Sicherheitsdienst, der die Richtlinien für die Benutzer steuert. Die lsass.exe ist dafür verantwortlich, dass nur angemeldete Administratoren auf alle Dateien Zugriff haben und für eingeschränkte Benutzer den Zugriff auf das Betriebssystem verhindert wird.
alg / alg.exe (**A**pplication **L**ayer **G**ateway), dieser Service ist Teil der Internet Connection Sharing (ICS) und wirkt mit, wenn mehrere Computer eine einzelne Internetverbindung nutzen. Zum anderen ist sie Teil der Internetverbindungsfirewall (ICF).
csrss / csrss.exe (**C**lient **S**erver **R**untime **S**ub**s**ystem) verwaltet und steuert die Fenster von Anwendungen sowie das Anlegen und Beenden von Threads (Funktionen) einer laufenden Anwendung.
services / services.exe ist der so genannte "Windows Service Controller" und für den reibungslosen Windowsbetrieb ausgesprochen wichtig. Der Prozess ist für den automatischen Start von Services und Dienstprogrammen beim hochfahren des Rechners zuständig. (Thema 3.63)
spoolsv / spoolsv.exe (Spooler SubSystem) sorgt dafür, dass Druckaufträge nacheinander an den Drucker gesendet und neue Druckaufträge geordnet in die Druckerwarteschlange eingereiht werden.
svchost / svchost.exe (**S**erv**i**ce**Host**) ist ein Systemprozess mit dessen Hilfe DLL - Dateien ausgeführt werden. Die svchost.exe ist mehrfach in Funktion (Threads). Im Task-Manager können nicht alle Prozesse namentlich getrennt aufgeführt werden. Wenn mit dem Eingabefenster *Start/Ausführen: cmd* eingetippt und mit *Return* gestartet wird, öffnet sich die *Eingabeaufforderung.* Im Eingabefenster wird der Befehl *Tasklist/svc | more* eingetippt und *svchost.exe* listet die einzelnen Prozesse auf.

winlogon / winlogon.exe ist der Anmeldedienst (Magina) von Windows. Wenn eine neue interne Hardwarekomponente eingeführt wird, stellt die winlogon.exe dies fest und sorgt dafür, dass bei erforderlicher, erneuter Produkt-Aktivierung von Windows XP diese von Microsoft bestätigt wird.
taskmgr / taskmgr.exe startet den Task-Manager,
ctfmon / ctfmon.exe gehört zu Microsoft Office. Sie überwacht offene Fenster und dient der Spracherkennung, sowie der zur Verfügungstellung alternativer Texteingabegeräte. Im übrigen kann das Programm auf dem PC sein, obwohl man gar kein OFFICE hat.
avgnt / avgnt.exe und **avguard /avguart.exe** startet, wenn der Benutzer das kostenlose Antiviren - Programm "AntiVir" verwendet.
locator / locator.exe (locator bedeutet RPC locator) wartet die Interprozesskommunikation zweier Rechner (RPC, Remote Procedure Call).
Neben diesen Windows-Systemprozessen werden auch Prozesse für spezielle vom Benutzer installierte Programme geladen, wie Nero-CD-Brenner, InCD, IrfanView, Adaware, TrojanerCheck, Google-Tools u.a.

Damit ist jedoch der Ladevorgang von Systemdateien noch nicht beendet. Die oben genannten Prozesse benötigen für ihre Arbeit sogenannte DLL (Dynamic Link Library). Das sind Programmbibliotheken, die in weit größerem Umfang in den Arbeitsspeicher geladen werden, als der Benutzer vermutet. Z.B sind ***svchost / svchost.exe*** und ***rundll32 / rundll32.exe*** Systemprozesse mit deren Hilfe DLL - Dateien ausgeführt werden. Es wird im Menü über *Start/Ausführen: Eingabefenster* eingeleitet. Z.B.: rundll32.exe shell32.dll, Control_RunDLL timedate.cpl u.a. Schließlich sind in Abhängigkeit der Benutzeraktivitäten immerhin ca. 300 Dateien geladen und in Arbeitsspeicher und Auslagerungsdatei in einem Umfang von etwa 300 MB gespeichert worden.

Es besteht aber auch die Gefahr, dass sich im Ladeprozess Schadprogramme, wie Viren, Würmer, Trojaner eingenistet haben. Z. B. ist **svchost2 / svchost2.exe** ein Virus / Spyware, der sich der Namensähnlichkeit mit der ***svchost.exe*** zu nutze macht, welcher ein Systemprozess ist. Auch der Wurm "W32.NIMDA.E@mm" kopiert sich als csrss.exe in Form einer Variablen in die entsprechende Datei!

Es stellt sich die Frage:
Welche Prozesse, die im Arbeitsspeicher als Systemkern von Windows XP gespeichert werden, sind für den Start des Betriebssystems unentbehrlich und welche können zunächst deaktiviert bleiben? Wie kann ich den Umfang der zu startenden Prozesse begrenzen, wenn sie gar nicht benötigt werden? Wie weiter oben bereits ausgeführt, hat sich der Umfang der startenden Treiber von Service Pack zu Service Pack erhöht und mancher stellt dann fest: „Mein Computer ist seit der Installation von Service Pack 3 langsamer geworden."

Auch jede neue Software ist berechtigt mittels **API** *(Application Program Interface)* Einträge in das Windowsbetriebssystem vorzunehmen, damit Befehle mit Hardwarekomponenten ausgeführt werden können und auf Datenbänke zugegriffen werden kann. Programme können deshalb nur mit Administratorrechten installiert werden.

Die Befehlsstelle für den Start aller Treiber, Prozesse und DLL ist die *Registry*, die im System versteckte Datenbank. Um den Start von entbehrlichen Systemdateien zu verhindern, muss diese nicht in erster Linie aus dem Windowsordner entfernt, sondern vor allem als Eintrag in der Registry gelöscht werden. Es gibt zwar Registry-Optimierer und –reiniger (cleaner), die aber die Entfernung von Registry-Einträgen automatisch und oft zum Schaden mancher Prozesse vollziehen. Zu bevorzugen ist jedoch eine benutzerspezifische Auswahl zur Reduzierung der Startprozesse, die allerdings entsprechende Sachkenntnis voraussetzt. Dazu müssen noch Erfahrungen gesammelt werden.

In erster Linie ist die Kenntnis der Startrampen in der Registry erforderlich, deren Existenz meist nur wenigen Benutzern bekannt sind. Ein Werkzeug (Tool), das die Startrampen analysiert, Startschlüsselnamen der Registry (mehr als 20) und die Dateinamen, Beschreibung, Herausgeber, Pfad usw. anzeigt ist *autoruns.exe* von www.sysinternals.com. (Bild) Damit sind auch Deaktivierungen, Entfernen und Exportieren von Registry-Einträgen möglich.