X.systems.press

X.systems.press ist eine praxisorientierte Reihe
zur Entwicklung und Administration
von Betriebssystemen, Netzwerken und Datenbanken.

Martin Grotegut

Windows Vista

Erste Auflage

Springer

Martin Grotegut

ISBN 978-3-540-38882-1 e-ISBN 978-3-540-38884-5

DOI 10.1007/978-3-540-38884-5

ISSN 1611-8618

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

© 2008 Springer-Verlag Berlin Heidelberg

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten waren und daher von jedermann benutzt werden dürften.

Einbandgestaltung: KünkelLopka, Heidelberg

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Vorwort

Wenn man den Vorschlag erhält, ein Buch zu schreiben, sind unabdingbare Voraussetzungen, das Thema genauestens zu kennen, eine Auswahl und Eingrenzung durchzuführen sowie diese didaktisch gut gemacht zu präsentieren.

Dieses Buch wendet sich daher an erfahrene IT-Spezialisten und -Spezialistinnen sowie andere technisch Interessierte, die ihre Kenntnisse um Windows Vista erweitern und ggf. durch Microsoft zertifizieren lassen, oder sich zumindest einen detaillierten Überblick über Windows Vista verschaffen möchten.

Im folgenden werden daher nicht etwa der Internet Explorer und das Media-Center in allen Details vorgestellt, sondern es wird auf den Einsatz und die Installation als Arbeitsstation in Unternehmen fokussiert und zahlreiche Tipps und Tricks aus der Praxis gegeben. Reine Serverfunktionalitäten werden nicht betrachtet. Dennoch wird Ihnen vermutlich das eine oder andere bereits bekannt sein – eine Berücksichtigung des leserinnen- und leserindividuellen Vorwissens war leider nicht möglich.

Im folgenden wird die endgültige Windows Vista Ultimate-Edition beschrieben, die als Vereinigungsmenge wirklich alle verfügbaren Funktionen der gesamten Windows-Vista-Familie beinhaltet. In anderen Vista-Versionen sind nicht alle hier beschriebenen Funktionen verfügbar.

Dieses Buch kann auch als Grundlage für die Vorbereitung auf die MCP-Prüfungen 70-620 und 70-623 verwendet werden. Unerlässlich dazu ist jedoch ein vollständiges Durchlesen sämtlicher Kapitel und einige praktische Übungen durchzuführen.

Ein komplexes Projekt wie die Erstellung eines Buches ist selbstverständlich kein Werk eines Einzelnen, sondern stets sind etliche Leute dabei involviert. So danke ich ausdrücklich meinem Lektor Herrn Hermann Engesser, den Lektoratsassistentinnen Frau Gabi Fischer und Frau Dorothea Glaunsinger sowie Frau Viktoria Salma und Herrn Michael Reinfarth für ihre Arbeiten, die zum Erscheinen dieses Buches unerlässlich waren und es erst ermöglicht haben.

Eventuell verbleibende Fehler gehen natürlich zu meinen Lasten. Solche Errata werde ich auf meiner Homepage (http://www.zbc-berlin.de/) veröffentlichen.

Dieses Buch erscheint etwas später als erwartet: Einer der Gründe dafür ist, dass der Autor das Erscheinen des Microsoft Windows-Vista-Ressource-Kits unbedingt abwarten wollte, um die aus seiner Sicht relevanten, und in der Regel sonst nur dort detailliert beschriebenen systemnahen Punkte des Betriebssystemherstellers in dieses Buch miteinzuarbeiten, um dann leider enttäuschter Weise feststellen zu müssen, dass jenes Werk aufgrund einer nicht endgültigen, Beta-Version von Vista geschrieben wurde und in ihm der Windows Server 2008 noch unter seinem früheren Codenamen „Longhorn“ bezeichnet und beschrieben wird.

Ein weiterer Grund für die Verzögerung besteht in der ausdrücklichen Ausrichtung dieses Buchs auch für die Vorbereitung auf die MCITP- und MCTS-Zertifizierungen für Windows Vista, denn Microsoft wird im März 2008 viele von ihr als veraltet angesehene Prüfungen stornieren, so dass abzusehen ist, dass es zwangsläufig zu einer Vielzahl von Rezertifizierungen von Leuten kommen wird, die in der aktuellen Technologie zertifiziert bleiben möchten. Um nichts Wichtiges auszulassen, konnte das Manuskript daher erst nach Erscheinen der genannten MCP-Examen dem Verlag übergeben werden.

Wenn Sie den Autor für Hinweise, Kritik, Vorschläge etc. kontaktieren möchten, können Sie das per E-Mail an die Adresse *MG@MGrotegut.de* gerne tun.

Berlin, im August 2007 Martin Grotegut

Inhaltsverzeichnis

1 Systemaufbau Windows Vista

Windows Vista ist die neueste Version der Windows-NT-Familie. Diese zeichnet sich durch hohe Stabilität und Sicherheit aus. Microsoft verspricht sogar, mit Windows Vista die robusteste und sicherste Windowsversion ausgeliefert zu haben. Aber wie wird dies realisiert? Windows Vista ist in zwei wichtige Bereiche unterteilt: Es gibt den Kernel-Modus und den Benutzermodus, die voneinander getrennt sind. Sehen wir uns diese Bestandteile einmal genauer an.

1.1 Der Kernel-Modus

In der oberen Hälfte des zur Verfügung stehenden Adressraums des Prozessors arbeiten in einem besonders geschützten Bereich die Kernel-Prozesse. Der direkte Zugriff auf die Komponenten, die Hardware des Systems ist Benutzerprozessen verwehrt und kann nur durch den Kernel selbst vorgenommen werden. Das bewirkt, dass das Betriebssystem zu jeder Zeit die volle Kontrolle über das gesamte Computersystem hat. Nicht erlaubte Zugriffe werden abgefangen, und falls ein Benutzerprozess abstürzen sollte, zieht dies nicht etwa das ganze System in Mitleidenschaft, sondern der betreffende Prozess kann einfach neu gestartet werden, ohne dass der Rechner an sich neu gestartet werden müsste. Der Kernel selbst besteht aus weiteren Unterfunktionen (siehe unten) und ist somit nicht *monolithisch*. Andererseits hat der Vista-Kernel aber auch nicht eine Microkernel-Architektur in Reinform, weil die Funktionen nicht geändert bzw. ersetzt werden können. Das von Microsoft hierbei realisierte Modell wird *Hybrid-Kernel* genannt. Aber blicken wir auf die einzelnen Unterfunktionen:

1.1.1 Die Hardwareabstraktionsschicht (HAL)

Nein, dies hat nichts mit dem durchgeknallten Computer aus „Odyssee im Weltraum“ zu tun: Durch die HAL (Hardware Abstraction Layer) werden sämtliche Geräte und Schnittstellen im System virtualisiert und hardwareabhängige Details wie Interruptcontroller, E/A-Schnittstellen etc. verbor-

gen. Kein Prozess oder Treiber (auch solche des Kernels selber) kann dadurch mehr direkt auf die Hardware zugreifen.

Die ursprüngliche Absicht war es, Unterschiede der verschiedenen Plattformen (Windows NT gab es auch mal für Power PC-, MIPS- und Alpha-Systeme sowie für Ein- und Mehrprozessorsysteme) auszugleichen und Programmierern eine homogene Programmierebene zu geben.

HALs gibt es nun nur noch als Mehrprozessorversionen für Intel x86-32-Bit, 64-Bit und Intel IA-64-Bit kompatible Systeme, die aber natürlich auch auf PCs mit nur einer CPU bzw. nur einem CPU-Kern funktionieren, wenn auch etwas langsamer als die früheren Uniprocessor-Versionen. Gleichfalls wurde die Unterstützung von Nicht-ACPI-fähigen (Advanced Configuration and Power Interface) Systemen durch eigene HALs eingestellt.

Sämtliche Funktionen sind in der Datei HAL.DLL enthalten.

1.1.2 Der Mikro-Kernel

Auf der HAL setzt der Mikro-Kernel (und auch die Kernel-Modus-Treiber, siehe unten) auf. Dieser besitzt Multiprozessor-Ablaufkoordinations-, Threadzeitsteuerungsfunktionen, (dadurch wird entschieden, welche Threads ausgeführt werden sollen und wie lange sie jeweils CPU-Zeit erhalten) und Interruptweiterleitungsfunktionen. Als *Threads* werden Unterfunktionen eines Prozesses (auch *Task* genannt) bezeichnet, die gleichzeitig ausgeführt werden können (mehrere CPUs vorausgesetzt). Ein Beispiel: Eine typische Office-Anwendung wie Microsoft Word führt während der Texteingabe (das ist *ein* Thread) permanent weitere Funktionen wie den Druckumbruch (damit der Schreiber bzw. die Schreiberin weiß, auf welcher Seite sie sich befinden), Rechtschreibkorrektur, Grammatikprüfung etc. aus.

Sämtliche Mikro-Kernel-Routinen sind in der Datei NTOSKRNL.EXE enthalten.

1.1.3 Kernelmodusgerätetreiber

Gerätetreiber, die exklusiv den physischen Zugriff auf die Ressourcen eines Geräts realisieren, müssen als Kernel-Modus-Treiber, welche dann in derselben Schutzebene wie das Betriebssystem ausgeführt werden, programmiert und digital signiert sein.

Dabei ist sorgfältige Entwicklung wichtig, denn ein Problem in einem beliebigen Kernelmodusgerätetreiber würde das gesamte System zum Absturz bringen.

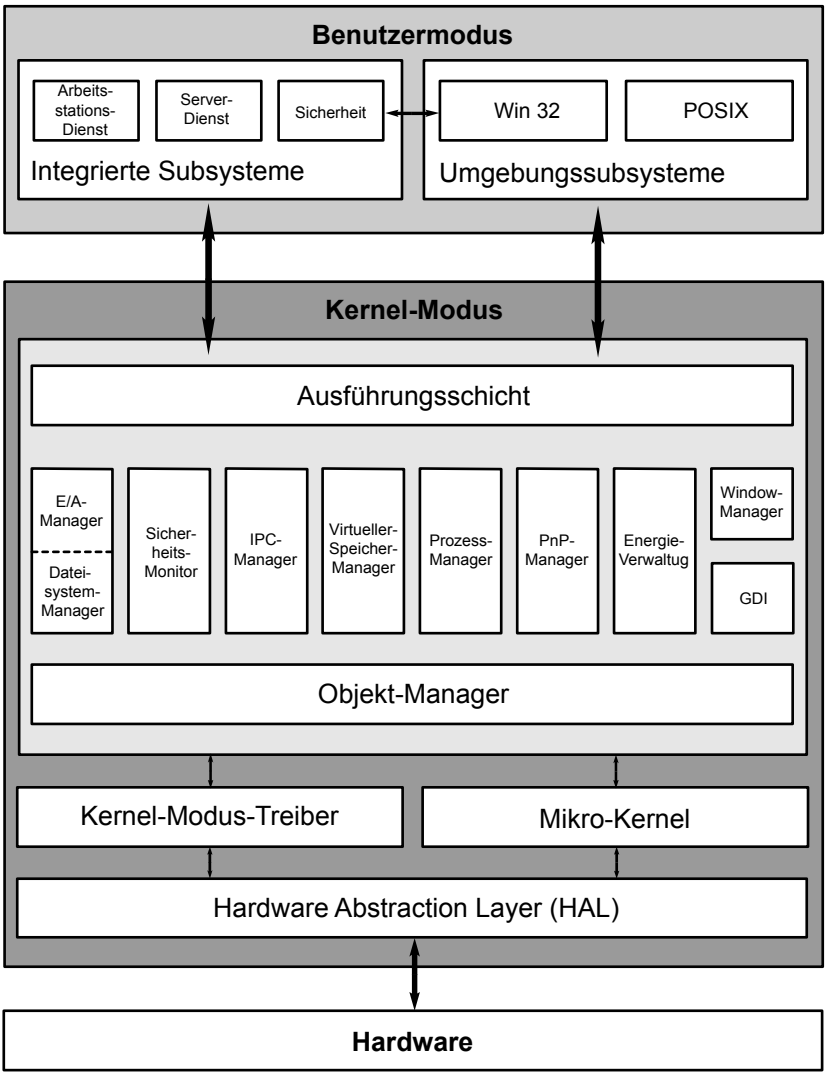

Abb. 1.1. Windows Vista Systemarchitektur

1.1.4 Die Ausführungsschicht (Executive)

Die Ausführungsschicht ist ein Bindeglied zwischen den Benutzermodus-Subsystemen und den anderen Kernel-Bestandteilen und ist damit ein Hauptbestandteil des Vista-Kernels.

Seine wichtigste Aufgabe besteht in der Kommunikation mit den Benutzermodus-Subsystemen und seinen eigenen Kernel-Subsystemen Objekt-Manager, IPC-Manager, E/A-Manager, VM-Manager, PnP-Manager, Sicherheitsmonitor, Power Manager und dem Windows Manager.[1]

1.1.5 Der Objektmanager

Der Objektmanager ist ein spezielles Subsystem der Ausführungsschicht, der für den Zugriff auf Objekte durch alle anderen Subsysteme zuständig ist. Für den Objektmanager sind alle Ressourcen des Systems Objekte. Dazu gehören physische Objekte (wie E/A-Schnittstellen oder ein Dateisystem) und logische Objekte (bsp. ein Verzeichnis oder eine Datei).

Durch den Objektmanager erscheinen alle Bestandteile von Windows Vista objektorientiert zu sein und der Zugriff hierauf wird durch Klassen und Methoden realisiert.

Andere wichtige Aufgabe des Objektmanagers sind, gleichzeitigen Zugriff auf Systemressourcen zu steuern, so dass es hierbei nicht zu Konflikten kommt, und den Speicher für Objektbeschreibungsstrukturen anzufordern und freizugeben.

1.1.6 Der E/A-Manager

Der Eingabe-/Ausgabe-Manager (engl.: Input/Output-Manager bzw. I/O-Manager) steuert die Kommunikation zwischen Benutzermodus-Subsystemen und den Kernel-Gerätetreibern. Sämtliche Ein- und Ausgabeanforderungen werden an ihn in geräteunabhängiger Form geschickt und von ihm an die Kernel-Modus-Gerätetreiber weitergeleitet, die dann mit den entsprechenden virtuellen, logischen und physischen Geräten kommunizieren. Falls es mehrere gleichzeitige Anforderungen gibt, liegt es in der Verantwortung der Treiber, eine Priorisierung und Reihenfolge festzulegen, in der sie an die E/A-Geräte weitergeleitet werden.

---

[1] Ein weiterer Bestandteil der Ausführungsschicht ist der Konfigurationsmanager, der Zugriffe auf die Registrierung koordiniert. Aufgrund dieser Funktion ist er gelegentlich in anderer Literatur als eigenständiger Teil aufgeführt.

Wenn Gerätetreiber mit anderen Gerätetreibern kommunizieren möchten, geschieht das gleichfalls über den E/A-Manager.

Der E/A-Manager arbeitet eng mit PnP-Manager (für das Hinzufügen und Entfernen von Geräten und ihren Treibern) und der Energieverwaltung (Unterstützung beim Wechsel in den Energiesparmodus und zurück) zusammen.

Unterfunktionen des E/A-Managers sind der Dateisystemmanager (engl.: *File System Manager*) und der Dateisystemcache. Letzterer kommuniziert dazu mit dem Virtuellen-Speicher-Manager.

Der E/A-Manager kümmert sich auch um die Kommunikation mit Systemen, die über Netzwerke miteinander verbunden sind.

Bei den Eingabe- und Ausgabeanforderungen wird zwischen *synchroner* und *asynchroner E/A* unterschieden: Bei der synchronen E/A sendet eine Anwendung eine E/A-Anforderung und wartet auf ihren Abschluss, der erfolgreich oder fehlerhaft sein kann, bevor sie weiterarbeitet. Bei asynchroner E/A, welche die Leistung einer Anwendung im allgemeinen erhöht, wartet sie nicht auf die Fertigstellung der Anforderung, sondern arbeitet währenddessen weiter. Insbesondere bei Leseoperationen muss die Anwendung sicherstellen, dass erst nach erfolgreicher Beendigung des Vorgangs auf den Dateipuffer zugegriffen wird. Hierzu sendet der E/A-Manager nach dem Abschluss der angefragten Operation eine Benachrichtigung, die auch einen Statuscode enthält.

Programmierer haben zudem die Möglichkeit, anzugeben, ob die Operationen seitens des E/A-Managers gepuffert oder ungepuffert erfolgen sollen bzw. es dem jeweiligen Gerätetreiber überlassen werden soll, ob Datenpuffer verwendet werden.

Für kleinere Datenblöcke (kleiner als 4 KB) empfiehlt sich die durch den E/A-Manager-gepufferte Lösung, für größere Datenmengen und DMA-Vorgänge dagegen die direkte E/A.

1.1.7 Der Sicherheitsmonitor (Security Manager)

Durch den im Kernel-Modus arbeitenden Sicherheitsmonitor[2] wird sichergestellt, dass auf sämtliche Ressourcen des Systems nur in der Art, wie sie durch ACLs (Access Control Lists, Zugriffssteuerungslisten) bestimmt wird, zugegriffen werden kann.

Zur Kommunikation mit der Local Security Authority (LSA), die im Benutzermodus arbeitet, verwendet der Sicherheitsmonitor LPCs (Local

[2] Er wird gelegentlich auch als Sicherheitsreferenzmonitor (SRM) bezeichnet.

Procedure Calls). Winlogon verwendet gleichfalls LPCs zur Kommunikation mit der LSA.

Eine wichtige Aufgabe des Sicherheitsmonitors ist die Erstellung von Zugriffstokens (engl.: Access Tokens), die u. a. Systemrechte enthalten.[3]

1.1.8 Der IPC-Manager

Der Interprocess Communication Manager (IPC Manager)[4] steuert die Kommunikation über RPC (Remote Procedure Call) zwischen Prozessen im Kernelmodus und solchen, die im Benutzermodus arbeiten. Prozesse verwenden dazu immer RPC-APIs, die wiederum so genannte *Pipes* für den Lese-/Schreibzugriff öffnen.

Wenn sich die Quelle und das Ziel auf demselben Rechner befinden, werden LPC (wie schon im Punkt 1.1.7 erwähnt) verwendet, und wenn möglich nicht durch den Versand von Ereignisnachrichten, sondern zur Leistungssteigerung durch Nutzung eines gemeinsamen Speicherbereichs.

1.1.9 Der Virtueller-Speicher-Manager

Dieser Kernel-Bestandteil (engl.: Virtual Memory Manager) verwaltet den gesamten physischen und den Speicherplatz, der durch die Auslagerungsdatei erzielt wird, und gibt ihn als virtuellen Speicher frei.

Jeder Prozess erhält einen eigenen, privaten virtuellen Adressraum. Dieser kann jeweils auch größer sein als die physisch installierte Speichermenge und bei 32-Bit-Systemen bis zu 2 bzw. 3 GB groß sein. Dazu wird die Auslagerungsdatei verwendet.

Nicht benötigte physische Speicherbereiche übergibt er dem Dateisystemcache, damit auf vor kurzem geöffnete Dateien schneller zugegriffen werden kann.

1.1.10 Der Prozess-Manager

Die Aufgabe des Prozess-Managers ist, den erfolgreichen Start und Beendigung von Prozessen und Threads sicherzustellen.

Dazu gehört auch die Anforderung und Freigabe von Speicher vom Virtuellen-Speicher-Manager.

---

[3] Näheres dazu finden Sie in Kapitel 7.

[4] In anderer Literatur wird dieser auch einfach nur als *Lokaler Prozeduraufruf* bezeichnet.

1.1.11 Der Plug-und-Play-Manager

Der Plug-und-Play-Manager fragt während des Systemsstarts die Ressourcenanforderungen (u. a. IRQs, E/A-Anschlüsse, RAM, DMA, busspezifische Ressourcen) der Geräte ab, prüft sie auf Überschneidungsfreiheit und weist ihnen dann die zu benutzenden Ressourcen zu. Außerdem ermittelt er, welche Treiber die jeweiligen Geräte benötigen und lädt diese in den Speicher.

Wenn während des Betriebs Geräte hinzugefügt oder entfernt werden, sorgt er für die entsprechenden Benachrichtigungen an die anderen Systemkomponenten und das Laden und Entladen von Gerätetreibern.

Dazu kommuniziert er auch mit dem Benutzermodus-PnP-Manager, der in der Datei *Umpnpmgr.dll* implementiert ist.

1.1.12 Die Energieverwaltung (Power Manager)

Ihre Aufgabe ist anhand der Energierichtlinie per ACPI[5] Geräte(funktionen) ein- und auszuschalten, damit der in der Richtlinie vorgegebene Leistungsgrad (energiesparend oder mit voller Leistung) eingehalten wird.

Wie Geräte nun konkret in einen energiesparenden Modus versetzt und aus ihm wieder aufgeweckt werden, ist Aufgabe der Gerätetreiber. Der zu einem bestimmten Zeit zu herrschende Zustand wird jedoch von der Energieverwaltung vorgegeben.

1.1.13 Der Window-Manager und GDI

Zu Windows NT 3.51-Zeiten noch im Benutzer-Modus arbeitend, sind die Funktionen Window Manager und GDI (Graphics Device Interface) zur Erhöhung der Leistung in den Kernel-Modus verschoben worden und in der Datei Win32k.sys realisiert.

Die Aufgaben des Windows Managers sind die Veranlassung der Darstellung von Fenstern und Menüs sowie die entsprechende Weiterleitung

[5] Abkürzung von *Advanced Configuration and Power Interface*. Die Spezifikation befindet sich bsp. auf http://acpi.info/spec.htm.
Systeme, die vor 1998 gebaut wurden, entsprechen häufig nur der Vorgängerspezifikation APM (Advanced Power Management). Auf ihnen kann Vista schon aus diesem Grund nicht ausgeführt werden – aber wahrscheinlich erfüllen so alte Geräte auch andere Mindestvoraussetzungen (siehe unten) nicht.

von Benutzeraktionen wie Maus- und Tastaturereignisse an die betereffenden Anwendungen weiterzuleiten.

Die Aufgabe des GDI ist, die Darstellung von Linien und Kurven zu veranlassen. Es leitet die entsprechenden Anforderungen an die entsprechenden Gerätetreiber (z. B. Bildschirm, Drucker etc.) weiter.

1.2 Der Benutzermodus

Im Benutzermodus werden zum einen sämtliche Prozesse, die ein Anwender gestartet hat, ausgeführt. Zum anderen aber auch Teile des Betriebssystems (auch als Integrierte Subsysteme bezeichnet).[6] Diese Prozesse sind untereinander und gegenüber dem Betriebssystem abgeschottet. Eine beliebige Anwendung, die versuchen sollte, auf den Adressbereich einer anderen Anwendung oder des Betriebssystems zuzugreifen, wird vom Betriebssystem unter Ausgabe einer Fehlermeldung beendet.

Eine Neuerung von Windows Vista sind Benutzermodus-Treiber.[7] Dieses sind Gerätetreiber (z. B. für Druck- und USB-Geräte wie eine Kamera), die im Benutzermodus ausgeführt werden, zwar dennoch nicht unmittelbar auf die Hardware selbst zugreifen dürfen, aber für deren Installation nicht mehr zwingend administrative Rechte erforderlich sind. Und falls ein solcher Gerätetreiber einmal abstürzen sollte, berührt es das Betriebssystem nicht. Nach der Installation eines UMDF-Treibers (User Mode Driver Framework) muss ein Rechner zudem nun in aller Regel nicht mehr neu gestartet werden.

---

[6] Ein Beispiel dafür ist der Sitzungs-Manager (engl.: *Session Manager*), der in der Datei Smss.exe implementiert ist und u. a. die Umgebungsvariablen setzt, ggf. vorhandene weitere Auslagerungsdateien öffnet und das Win32-Subsystem (Csrss.exe) und Winlogon (eben falls im Benutzermodus) startet.
Danach ist er für den Start neuer Terminal-Server-Sitzung und ggf. weiterer Subsysteme (derzeit kann das eigentlich nur das POSIX-Subsystem sein) zuständig.
Andere Funktionen, die im Benutzermodus arbeiten sind die *Local Security Authority* (Lsass.exe) und der Dienststeuerungs-Manager (Services.exe).

[7] Das User Mode Driver Framework ist danach auch für Windows XP veröffentlicht worden.

1.3 Dienste

Ein guter Teil der Betriebssystemfunktion von Windows Vista wird durch Dienste realisiert. Dienste starten typischerweise mit dem Betriebssystem und arbeiten bis zum Herunterfahren des Systems im Hintergrund. Hierzu muss kein Benutzer angemeldet sein. Microsoft hat mit Vista aber auch die Arbeitsmöglichkeit als Benutzerdienst eingeführt. Letztere arbeiten dann im Sicherheitskontext des angemeldeten Benutzers.

Dienste (und auch Gerätetreiber) werden beim Start von Vista durch den Service Control Manager (SCM , dt.: Dienststeuerungs-Manager) geladen und gestartet. Dieser Teil des Betriebssystems ist somit direkt für das Arbeiten der Dienste zuständig.

Sämtliche Dienste sind (zusammen mit den Geträtetreibern) im Registrierungspfad HKLM\SYSTEM\CurrentControlSet\Services aufgeführt (siehe unten).

Dienste können voneinander abhängen. Ein Beispiel: Der Arbeitsstationsdienst könnte nicht starten, wenn ein Netzwerkprotokolldienst wie TCP/IP (noch) nicht zur Verfügung steht. Das ist insbesondere bei der neuen Dienststartart *Automatisch-Verzögerter Start* zu beachten, die den betreffenden Dienst nachrangig und mit niedrigster Priorität startet. Diese neue Startart kann aber nicht wirkungsvoll für solche Dienste spezifiziert werden, von denen andere Dienste abhängen (siehe unten). In so einem Fall würde der SCM den betreffenden Dienst automatisch sofort starten. Falls Benutzerprogramme auf einen automatisch-verzögert startenden Dienst angewiesen sind, gibt es Fehlermeldungen, wenn der Dienst dann noch nicht gestartet ist.

Windows Vista führt als ein weiteres neues Feature Abhängigkeiten auch beim Herunterfahren ein, damit Dienste, die in einer bestimmten Reihenfolge heruntergefahren werden müssen, ohne Probleme zusammenarbeiten können. Vor Windows Vista war der Versand der Herunterfahrensmeldungen an die Dienste vom Betriebssystem zufällig. Dieses wird jetzt durch den Registrierungsschlüssel (siehe unten) HKLM\System\CurrentControlSet\Control\PreshutdownOrder="Shutdown Order", der vom Typ REG_MULTI_SZ sein muss, gesteuert. Die Dienstnamen sind als Werte der Shutdown-Order aufgeführt.

Apropos Herunterfahren: Neu ist auch das Feature *Herunterfahrenvorankündigung*: Für Dienste, die das möchten, schickt der SCM drei Minuten (Voreinstellung und jedoch durch den Dienst änderbar) vor dem eigentlichen Herunterfahren-Befehl eine Vorankündigung, so dass Dienste, die vergleichsweise länger als andere Dienste benötigen, ihre jeweils erforderliche Zeit bekommen um zu stoppen. In früheren Windows-Versionen

konnten beliebige Dienste (und auch Anwendungen) außerdem das Herunterfahren eines Systems verhindern. Damit ist nun auch Schluss: Wenn der Benutzer Vista anweist, das System herunterzufahren, kann man sich nun auch darauf verlassen, dass es gemacht wird. Die Zeiten, zu denen man nach einer Reise am Ziel angekommen feststellte, dass die Notebook-Batterie fast leer und auf dem Display ein Fenster zu sehen ist, in dem gefragt wird, ob man wirklich sicher sei, das Programm XY zu beenden, sind nun vorbei.

1.4 Adressraum (32-Bit/64-Bit) und VMM (Swap)

In den 32-Bit-Versionen von Vista (siehe unten) steht ein Gesamtadressraum von 2^{32} (das sind ca. 4 Mrd.) Speicherstellen (oder 4 GB) zur Verfügung. Von diesem Adressraum ist die eine Hälfte (2 GB) für Benutzerprozesse, die jeweils bis zu 2 GB groß werden dürfen, reserviert und die andere Hälfte für das Betriebssystem. In letzterem ist auch der Speicherraum für PCI-Karten, die *Memory-Mapped*-I/O verwenden oder eigenes RAM mitbringen, untergebracht.

Mehr als 4 GB RAM kann ein 32-Bit-System nicht adressieren.[8]

In einem speziellen Betriebsmodus, dem 3-GB-Modus, der durch einen Schalter in der Boot.Ini-Datei (s. u.) aktiviert werden konnte und nun über BCD-Einstellungen bei Bedarf aktiviert werden muss, stehen speziell dafür geschriebenen Anwendungen wie Microsoft SQL-Server oder Microsoft Exchange-Server 3 GB zur Verfügung. Das OS muss dann mit nur einem Gigabyte auskommen.

Angesichts des wachsenden Speicherhungers (und glücklicherweise fallenden Speicherpreisen) sind die nächsten Meilensteine 64-Bit-Betriebssysteme. Zwar stehen diesen auch keine 2^{64} Bytes RAM zur Verfügung, denn da sprechen elektronische Hindernisse dagegen, aber immerhin bis zu 128 Gigabyte sind möglich.

Bei einem 64-bittigen Windows müssen alle Gerätetreiber ebenfalls 64-bittig programmiert sein, Anwendungen jedoch nicht zwingend, weil sie ähnlich dem vorherigen WOW32 (Windows on Windows32) für 16-Bit-Applikationen in einer 32-Bit-Umgebung bei Vista nun im WOW64 auch

[8] Eine Ausnahme hiervon bilden Programme wie der SQL-Server, die AWE (Address Windowing Extensions) verwenden können, bei denen nacheinander weitere Speicherbereiche in einem Speicherfenster eingeblendet werden können (die Anwendung ist selbst für die Zuordnung von virtuellem und physischem Speicher verantwortlich). Aber auch mit dieser Technologie ist der gleichzeitig adressierbare Adressraum auf 4 GB begrenzt.

als 32-Bit-Applikation auf einem 64-Bit-Windows ausgeführt werden können. Selbstverständlich bleibt jede 32-Bit-Applikation dabei auf max. 2 GB RAM beschränkt.

16-Bit-Applikationen aus der Windows-3.x-Ära können auf einem 64-Bit-Windows nicht mehr ausgeführt werden, weil Microsoft dafür kein Subsystem mehr anbietet.[9]

In einer 64-Bit-Umgebung sind die automatische Registrierungs- und Systemverzeichnisumleitung für Benutzer nicht verfügbar. Ebenso die PAE (Physical Address Extensions) - die sind bei dem Adressumfang nicht mehr nötig.

Aktuelle Prozessoren sind nunmehr mit 64-Bit-Erweiterungen versehen, was den Umstieg einerseits erst ermöglicht und andererseits für die Zukunftssicherheit wichtig ist: Microsoft wird zwar bis auf weiteres Client-Betriebssysteme wie Windows Vista (und möglichen Nachfolgern) für 32-Bit-Systeme anbieten und auch der Windows-Server 2008 wird noch 32-bittig verfügbar sein.

Microsoft Exchange 2007, Windows Server 2008 Small Business Version und den Windows Server 2008 R2 wird den Ankündigungen von Microsoft zufolge es nur noch als 64-Bit-Versionen geben.

Sehen wir uns doch im nächsten Abschnitt einmal an, welche Versionsvielfalt allein bei Windows Vista existiert.

1.5 Windows-Vista-Versionen

Bei den Vista-Versionen hat Microsoft ganze Arbeit geleistet: In stolzen, mindestens 14 (!) unterschiedlichen Versionen[10] ist Vista jeweils pro Sprache erschienen.

Die *kleinste* und preiswerteste, deutsche Version ist *Windows Vista Home Basic*. Sie ist der direkte Nachfolger der Windows XP Home Edition. Aus dem Namen wird schon das von Microsoft gedachte Einsatzgebiet deutlich: Für den typischen Heim-PC. So beinhaltet die Home Basic Version Funktionen wie Movie Maker und Jugendschutz, die für ein Unternehmensumfeld weniger wichtig sind.

Die nächst höhere Version ist *Windows Vista Home Premium*. Sie beinhaltet alles aus der Home Basic Edition jedoch zusätzliche Funktionen wie Aero Glass, Tablet PC, Side Show und das überarbeitete Media Center. Es

[9] Gleiches gilt zwangsläufig für 16-Bit-Treiber.

[10] Eventuell kommen noch spezielle koreanische Versionen, die mit K bzw. KN gekennzeichnet sind, auf den dortigen Markt. Endgültige Informationen darüber gab es bei der Erstellung dieses Buchs jedoch nicht.

ist davon auszugehen, dass diese Version die am häufigsten verwendete Version von Windows Vista ist.

Speziell für Unternehmenskunden gibt es die Versionen *Vista Business* und *Vista Enterprise*. Erstere ist der Nachfolger von Windows XP Professional und wird vorinstalliert sowie als eigenständige Version erhältlich sein. Die Enterprise-Version wird hingegen nur an Großunternehmen, die Rahmenverträge mit Microsoft abgeschlossen haben, ausgeliefert.

Die sprichwörtlich „eierlegende Wollmilchsau" ist die *Windows Vista Ultimate Edition*, die sämtliche Funktionen aller oben genannten Versionen enthält, und (seit Ende Januar 2007) weitere spezielle, über Windows Update herunterladbare Ultimate Extras wie ein BitLocker-Konfigurationsprogramm, Speicherung der EFS- und BitLocker-Schlüssel in Microsoft Digital Locker, Poker-Spiel, DreamScore (mit dem sich ein Video als Arbeitsoberflächenhintergrund einstellen lässt) bietet. Sie ist auch die einzige Version für Endkunden, die sowohl als 32-Bit- als auch als 64-Bit-Version ausgeliefert wird. Andere Versionen liegen auch 64-bittig sowie auf fünf CD-ROMs vor, müssen aber von Microsoft gegen geringe Versandkosten bestellt werden.

Jedoch sind nicht alle Voll- und Upgradeversionen für Endkunden als *Retail*-Version (auch unter der Bezeichnung *Boxed* bekannt) im Ladenregal des örtlichen Computerhändlers zu finden, denn über vorstehende Aufzählung hinaus, gibt es außerdem eine (nur in Entwicklungsländern erhältliche) *Windows Vista Starter Edition*, Versionen für 64-Bit-Prozessoren, OEM-Versionen und von Vista Home Basic und Business gibt es aufgrund von EU-Vorschriften auch solche ohne Microsoft Media Player. Diese haben ein angehängtes ‚N' im Namen.

Für Heimanwender wird die Retail-Installations-DVD mit den Versionen Vista Home Basic, Vista Home Premium und Vista Ultimate ausgeliefert. Ein kostenpflichtiges Upgrade von einer „kleineren" Vista- auf eine „größere" Vista-Version ist mittel eingebauter Upgrade-Funktion möglich. Der Vorteil: Es entfällt die früher in so einem Fall notwendig gewesene Neuinstallation des Betriebssystems.

Nachfolgend sind die verschiedenen Versionen und ihre Hauptunterschiede dargestellt:

- Windows Vista Home Basic
  - (Nachfolger der XP Home Edition)
  - Gleichzeitige, eingehende Netzwerkverbindungen: 5
  - Internetverbindungsfreigabe
  - Movie Maker
  - Max. 4 (32-Bit) / 8 GB (64-Bit) RAM
  - Max. 1 CPU-Chip (mit beliebig vielen Kernen)

- Jugendschutz
- Remotedesktop (Nur Client)

- Windows Vista Home Premium
  - Wie Windows Vista Home Basic, plus:
  - Windows Aero Glass-Oberfäche
  - Tablet-PC-Funktionen
  - SideShow
  - Windows Media Center-Funktionen
  - DVD Maker
  - Movie Maker HD
  - Zusätzliche Spiele
  - Gleichzeitige, eingehende Netzwerkverbindungen: 10
  - Mobility Center
  - Synchronisation PC-to-PC
  - Max. 4 (32-Bit) /16 GB (64-Bit) RAM
  - Dia-Show

- Windows Vista Business
  - (Nachfolger von Windows XP Professional)
  - Wie Windows Vista Home Basic, plus:
  - Windows Aero Glass-Oberfäche
  - SideShow
  - Tablet-PC
  - Domänen-Mitgliedschaft
  - Internet Information Server 7
  - Gleichzeitige, eingehende Netzwerkverbindungen: 10
  - Remotedesktop (Client und Host)
  - P2P Meeting Place
  - Mobility Center
  - Client für Windows-Fax-Server
  - Synchronisation PC-to-PC
  - Max. 4 (32-Bit) /128 GB (64-Bit) RAM
  - Max. 2 CPU-Chips (mit beliebig vielen Kernen)
  - NTFS-Schattenkopien

- Windows Vista Enterprise
  - (Nur für Großkunden erhältlich)
  - Wie Windows Vista Business, plus:
  - BitLocker
  - Virtual PC Express

- Unix-Subsystem (SUA)
- Multi-Language-Kit

- Windows Vista Ultimate Edition
  - Diese Version enthält alle Vista-Funktionen und ist insoweit eine Kombination aus Windows Vista Home Premium und Windows Vista Enterprise.
  - Es gibt aber exklusive Windows Vista Ultimate Extras, die nur von Anwendern und Anwenderinnen dieser Version von der Microsoft-Website heruntergeladen werden können.

Zusätzlich gibt es von allen Versionen, außer der Starter-Edition, 64-Bit-Versionen. Der Installationsschlüssel ist sowohl für die 32- als auch die 64-Bit-Version gültig, es darf aber nur eine von den beiden installiert werden. Die 64-Bit-Versionen zeichnen sich durch folgende Unterschiede aus:

- Unterstützung von wesentlich mehr RAM
- Kernel-Treiber müssen 64-bittig programmiert und digital signiert sein
- Unterstützung für 64-Bit und 32-Bit-Software, aber nicht mehr für 16-Bit-Software und PAE (Physical Address Extensions)

- (Windows Vista Starter Edition)
  - Nur in Entwicklungsländern erhältlich
  - Beschränkung auf drei gleichzeitige Applikationen
  - Maximal 1024 x 768 Punkte Bildschirmauflösung
  - Keine Netzwerkfreigaben
  - Maximal 256 MB RAM

Ein Upgrade ist nur von XP und einer „kleineren“ Version von Windows Vista möglich, nicht jedoch von Windows 2000 und früher! Hierbei erfordern aber die Vista-Home-Versionen auch die frühere XP-Home-Version und die Vista-Business-Variante die Professional-Version von XP.

Wenn ein Upgrade von einer anderen Version (z. B. Windows NT oder Windows 2000) gewünscht wird, muss erst ein Zwischenschritt über Windows XP gemacht werden, ehe dann in einem zweiten Upgrade auf Vista aktualisiert werden kann.

1.6 Die Registrierung und ihre Verwaltung

Die Registrierung von Windows Vista beinhaltet wichtige Einstellungen und Zuordnungen einer Windows-Installation und ihrer installierter Programme. In früheren Windows-Versionen wurde dies mit textbasierten .Ini-Dateien vorgenommen, auch andere Systeme benutzen dazu entsprechende textbasierte Konfigurationsdateien. Abgesehen von der früheren Windows-64-KB-Größenbeschränkung haben textbasierte Konfigurationsdateien viele Nachteile: Die Speicherung und Auswertung der Einträge erfolgt üblicherweise nicht binär, sondern in einem Textformat. Das erlaubt zwar die Bearbeitung mit einem beliebigen Texteditor, hat aber Performancenachteile, weil alles erst von Text zu binären Daten gewandelt werden muss. Außerdem ist eine direkt weiterverarbeitbare, binäre Speicherung von Informationen üblicherweise nicht vorgesehen. Des weiteren können Lese- und Schreibberechtigungen sowie Überwachungseinstellungen nur auf Dateiebene, nicht aber auf Eintragsebene gesetzt werden.

Diese Nachteile hat die Windows-Registrierung (engl.: *Registry*) nicht. Sie wird transaktionsunterstützt und in einem binärem Format gespeichert, so dass ihre Inhalte direkt und ohne Konvertierung weiterverarbeitet werden können.

Die Registrierung selbst gliedert sich in mehrere Zweige: Die wichtigsten sind: HKLM (HKEY_LOCAL_MACHINE), HKU (HKEY_USERS), HKCU (HKEY_CURRENT_USER), HKCR (HKEY_CLASSES_ROOT) und HKCC (HKEY_CURRENT_CONFIG).[11]

Ein *Registry Hive* ist so etwas wie eine Unterteilung der Registrierung als Ganzes in mehrere Teile. Denn obwohl die Registrierung (z. B. im Registrierungs-Editor) als ein durchgängiges und hierarchisches System von Einstellungen aussieht, ist sie technisch in einige Einzeldateien aufgeteilt.[12] Wichtige Dateien finden sich im Verzeichnis %SystemRoot%\System32\config, %SystemDrive%\Users sowie in %SystemDrive%\Boot.

Zum Ansehen und Ändern der Registrierung wird im allgemeinen der Registrierungs-Editor (Regedit.exe) benutzt (siehe Abb. 1.2).

---

[11] Es gibt noch einen weiteren, der als HKEY_PERFORMANCE_DATA (HKPD) bezeichnet wird und lokalen sowie entfernten Zugriff auf die Leistungsindikatoren eines Systems bietet. Der Zugriff erfolgt über die Registrierungs-APIs, im Registrierungs-Editor wird dieser Stammschlüssel nicht angezeigt.

[12] Dieses kann man sich in dem Zweig HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist genau ansehen: Hier ist genau aufgeführt, welcher Teilregistrierungszweig durch welche Datei realisiert ist.

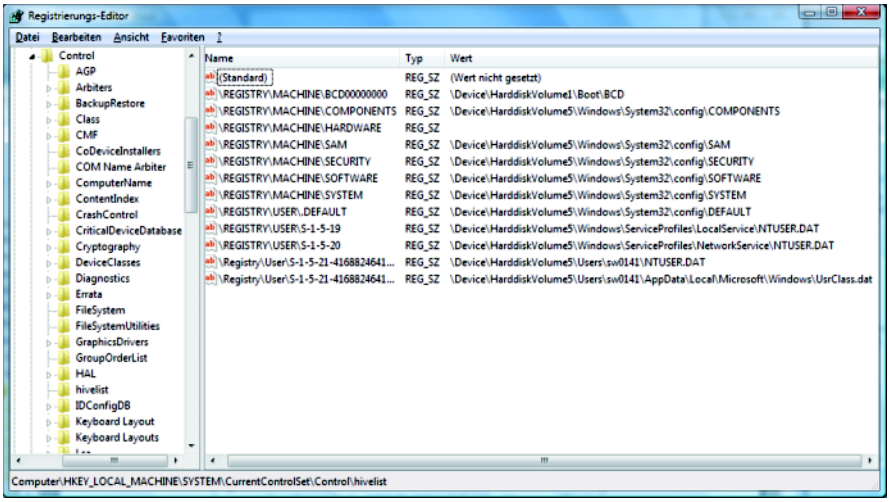

Abb. 1.2. Der Registrierungs-Editor

Aber auch der Reg.exe-Befehl und das Ausführen von Dateien mit der Endung .REG können dafür verwendet werden. Für Softwareentwickler stehen außerdem entsprechende Programmierschnittstellen (Application Program Interfaces, APIs) zur Verfügung.

Manchmal werden der Registrierung umgangssprachlich magische Kräfte zugesprochen („Da musste einfach die Registry ändern...“). Von solchen pauschalen „Empfehlungen“ ist eigentlich nur abzuraten: Erstens sollte man schon ganz genau wissen, was ein bestimmter Eintrag für Auswirkungen hat, zweitens ist, wenn eine Änderung auch über GUI-Tools möglich ist, diese vorzuziehen, weil sie andere, mitbetroffene Schlüssel ebenfalls ändert, und drittens können für die meisten Änderungen Gruppenrichtlinien verwendet werden. Nur wenn die letzteren beiden nicht zum gewünschten Ziel führen, bzw. Einträge nicht existieren und (z. B. aufgrund eines Hinweises in einem Knowledge-Base-Artikel) hinzugefügt werden müssen, sollte man eine direkte Änderung der Registrierung in betracht ziehen, denn unsachgemäße Änderungen können dazu führen, dass ein System nicht mehr startet!

Der Registrierungs-Editor lässt auch die Änderung eines Remote-Systems zu – allerdings stehen dann nur die Zweige HKLM und HKEY_Users zur Verfügung. Das reicht dies aber auch völlig aus, denn vieles, was als scheinbar eigenständige Struktur abgebildet wird, ist tatsächlich nur eine Verknüpfung auf andere Teile der Registrierung: So ist HKCU ein Unterschlüssel von HKEY_Users, HKCR und HKCC sind solche von HKLM,

und der Hardware-Baum wird nicht etwa dauerhaft gespeichert, sondern bei jedem Windows-Start dynamisch ermittelt und aufgebaut.

Die administrativen Vorlagen einer Gruppenrichtlinie sind eigentlich nur so etwas wie ein etwas komfortablerer Registrierungseditor. Die neuen .ADMX-Dateien sind nun XML-basiert.

In Tabelle 1.1 sehen Sie sämtliche Eintragstypen der Registrierungsdatenbank:

Tabelle 1.1. Registrierungsschlüssel

Typnr.	Bezeichnung	Inhalt
0	REG_NONE	Nichts. REG_NONE ist ein Platzhalter, wenn der richtige Typ noch nicht bekannt ist. Werden dennoch Daten hinterlegt, werden diese im Registrierungseditor als Typ REG_BINARY behandelt.
1	REG_SZ	Eine Zeichenkette (String). Sie wird mit dem Null-Zeichen terminiert.
2	REG_EXPAND_SZ	Eine Zeichenkette, die Umgebungsvariablen (z. B. %PATH%) enthalten darf. Bei der Auswertung des Registry-Eintrags wird zuerst der Inhalt der betreffenden Umgebungsvariable ausgelesen und anstelle von %...% verwendet.
3	REG_BINARY	Ein Binärwert.
4	REG_DWORD	Ein 32-Bit-Wert.
4	REG_DWORD_LITTLE_ENDIAN	Ein 32-Bit-Wert im Little-Endian-Format. Dieses wird u. a. von Intel-Prozessoren verwendet und ist gleichbedeutend mit dem REG_DWORD-Typ (weil Windows für Little-Endian-Prozessoren optimiert geschrieben wurde). Daher auch dieselbe Typnummer dieses Schlüssels. Im Little-Endian-Format wird ein Wert im Speicher mit dem niederstwertigen Oktett beginnend („das kleine Ende“) gespeichert: Bsp. der Wert 0x12345678 als (0x78 0x56 0x34 0x12).
5	REG_DWORD_BIG_ENDIAN	Ein 32-Bit-Wert im Big-Endian-Format. Im Big-Endian-Format werden die höchstwertigen Oktetts zuerst, und die niederwertigen

		Oktetts einer Hexadezimalzahl danach gespeichert. (Der Wert 0x12345678 wird im Big-Endian-Format als (0x12 0x34 0x56 0x78) gespeichert.) Dieses Format wird u. a. von Motorola-Prozessoren verwendet.
6	REG_LINK	Reserviert.
7	REG_MULTI_SZ	Mehrere Null-terminierte Zeichenketten. Das Ende der Liste wird durch eine Null-Zeichenkette gekennzeichnet.
8	REG_RESOURCE_LIST	Eine Geräte-Treiber-Ressourcenliste. Diese wird im Hardware-Hive verwendet und beinhaltet eine Reihe von verschachtelten Arrays, die eine Liste von Ressourcen enthalten, die Hardware-Gerätetreiber oder eines der physischen Geräte, die dieser steuert. Diese Daten werden vom System während des Starts erkannt und in den \ResourceMap-Baum geschrieben. Sie werden im Registrierungseditor als Binärwerte (REG_BINARY) dargestellt.
9	REG_FULL_RESOURCE_DESCRIPTOR	Eine Reihe von verschachtelten Arrays, die eine Ressourcenliste eines physischen Gerätes enthalten. Diese Daten werden vom System während des Starts erkannt, werden in den \HardwareDescription-Baum geschrieben und im Registrierungseditor als Binärwerte (REG_BINARY) dargestellt.
10	REG_RESOURCE_REQUIREMENTS_LIST	Eine Reihe von verschachtelten Arrays, die eine Liste aller möglichen Ressourcen darstellt, die ein Gerätetreiber oder der physischen Geräte, die er steuert, enthält. Das Betriebssystem schreibt eine Teilmenge dieser Liste in den \ResourceMap-Baum. Diese Daten werden vom System während des Starts erkannt und im Registrierungseditor als Binärwerte (REG_BINARY) dargestellt..
11	REG_QWORD	Ein 64-Bit-Wert
11	REG_QWORD_LITTLE_ENDIAN	Ein 64-Bit-Wert, der im Little-Endian-Format gespeichert wird. Dies entspricht dem REG_QWORD-Typ und erhielt dieselbe Typnummer wies dieser.