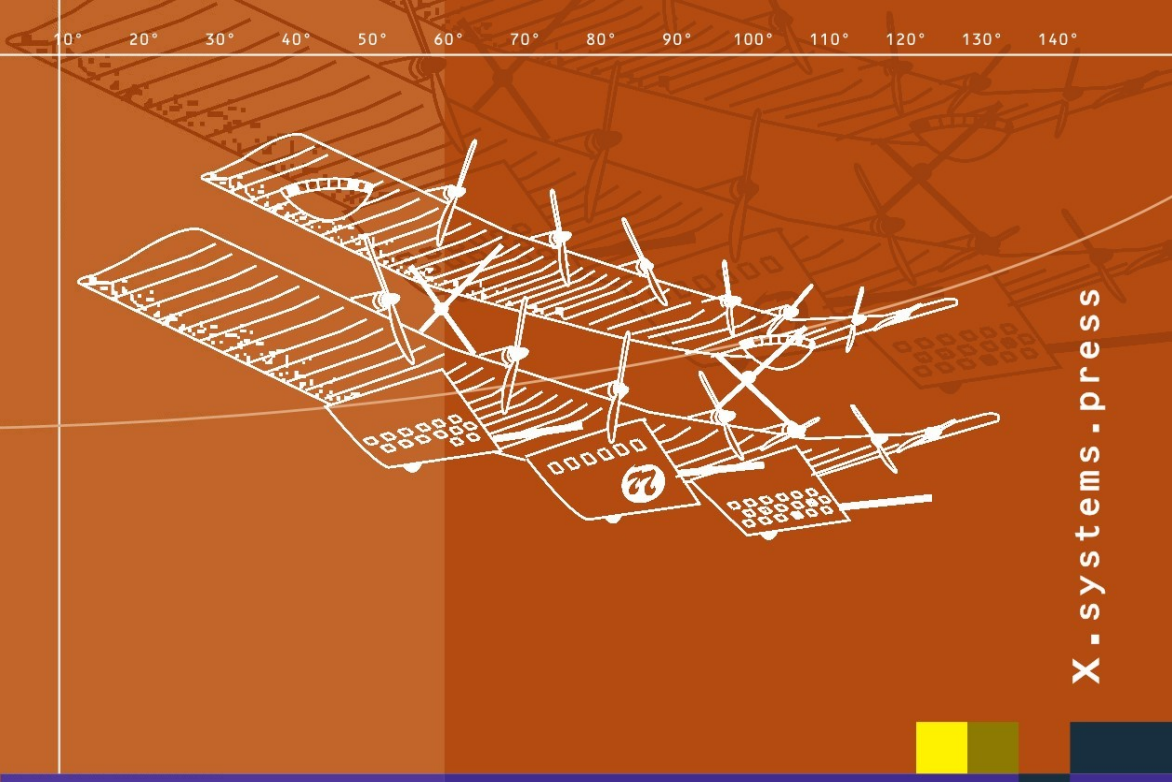

X.systems.press

Martin Grotegut

Windows 7

in Unternehmensnetzen mit Service Pack 1, IPv4, IPv6

Zur Vorbereitung für MCP 70-680 und Selbststudium

Springer

X.systems.press

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

Martin Grotegut

Windows 7

in Unternehmensnetzen mit Service Pack 1, IPv4, IPv6

Springer

ISSN 1611-8618
ISBN 978-3-642-01034-7 e-ISBN 978-3-642-01035-4
DOI 10.1007/978-3-642-01035-4
Springer Heidelberg Dordrecht London New York

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

Einbandentwurf: KuenkelLopka GmbH

Gedruckt auf säurefreiem Papier

Springer ist Teil der Fachverlagsgruppe Springer Science+Business Media (www.springer.com)

Vorwort

Liebe Leserin, lieber Leser,

mit Windows 7 ist ein würdiger Nachfolger von Windows Vista und auch Windows XP erschienen. Viele Funktionen der Vorgängerversionen wurden überarbeitet und ergänzt, sowie etliches hinzugefügt. Dabei wurde das Betriebssystem verschlankt, so dass es nun zum einen auch auf Netbooks eingesetzt werden kann und zum anderen sogar etwas schneller arbeitet als Windows XP. Durch einige Aspekte (Unterstützung von mehr als zwei CPU-Kernen, DirectX 11, etc.) ist es ihm technologisch zudem auch klar überlegen.

Dieses Buch beschreibt nicht etwa eine vorläufige, Beta-Version, sondern die endgültige Windows 7 Ultimate-Version mit installiertem Service Pack 1. Dabei wird auf die Client-Seite fokussiert, das Server-Backend wird nicht näher betrachtet. Es ist mir wichtig darauf hinzuweisen, denn einige Funktionen von Windows 7 (u. a. BranchCache und DirectAccess) können nur zusammen mit dem Windows Server 2008 R2 eingesetzt werden und werden daher zwar beschrieben, aber nicht detailliert betrachtet.

Mittlerweile ist sehr wichtig geworden, Kenntnisse über IPv6 zu haben. Deshalb beschreibe ich in dem Kapitel über Netzwerke (Kapitel 8) dieses Protokoll in seinen Grundzügen.

Dieses Buch wendet sich außerdem an den bzw. die erfahrene(n) Windows-Administrator(in) in einer Unternehmensumgebung und an diejenigen (auch Neueinsteiger), welche die MCP-Prüfung 70-680 (MCTS: Windows 7 Konfiguration) absolvieren möchten. Daher werden nicht etwa der Windows Explorer und der Windows Media Player etc. in allen Details vorgestellt, sondern der Fokus liegt auf dem professionellen Einsatz in kleinen, mittelständischen und großen Unternehmen.

Durch die jahrelange Trainings- und Projekterfahrung habe ich sehr detaillierte Kenntnisse des Alltags und der Bedürfnisse der Administration von Netzwerken in etlichen Unternehmen vielerlei Branchen gewinnen können, die in dieses Buch eingeflossen sind.

Als jüngstes meiner Bücher über Windows-Client-Betriebssysteme habe ich Anregungen und Wünsche meiner Leserinnen und Leser über die vorigen Versionen, die ich erhalten habe, bei der Erstellung berücksichtigt.

Wenn Sie mich kontaktieren möchten, können Sie das unter meiner E-Mail-Adresse MG@MartinGrotegut.de gerne tun.

An der Erstellung dieses Buchs sind außer mir als dem Autor viele andere Leute beteiligt gewesen: Mein ausdrücklicher Dank geht an das Springer-Verlag IT-Lektorat und an meine Ehefrau für die Durchsicht des Manuskripts sowie ihre stetige Unterstützung in allen Phasen der Erstellung dieses Werks.

Eventuelle Fehler gingen aber selbstverständlich zu meinen Lasten. Entsprechende Errata würde ich dann auf meiner Website (http://www.zbc-berlin.de) veröffentlichen.

Ich wünsche Ihnen viel Spaß beim Lesen, und dass Sie möglichst viele Informationen und Anregungen aus diesem Buch über Windows 7 entnehmen können.

Martin Grotegut

Inhaltsverzeichnis

Abkürzungsverzeichnis

3DES ..... Triple Data Encryption Standard
AACS ..... Advanced Access Content System
Abbr ..... Abbruch
ACE ..... Access Control Entry
ACL ..... Access Control List
ACPI ..... Advanced Configuration and Power Management Interface
AD ..... Active Directory
ADMA ..... Advanced Direct Memory Access
Aero ..... Authentic, Energetic, Reflective and Open
AES ..... Advanced Encryption Standard
AH ..... Authentication Header
ALCP ..... Advanced Local Procedure Call
ALG ..... Application Layer Gateway
Alt ..... Alternate
AMD ..... Advanced Micro Devices
API ..... Application Programming Interface
ARP ..... Address Resolution Protocol
ASCII ..... American Standard Code for Information Interchange
ASP ..... Active Server Pages
AuthIP ..... Authenticated Internet Protocol
AWE ..... Address Windowing Extensions
AxIS ..... ActiveX Installer Service
BASIC ..... Beginner's All-purpose Symbolic Instruction Code
BCD ..... Boot Configuration Data
BDD ..... Business Desktop Deployment
BDE ..... BitLocker Drive Encryption
BIOS ..... Basic Input/Output System
Bit ..... Binary digit
BITS ..... Background Intelligent Transfer Service
BKS ..... Benutzerkontensteuerung
BootP ..... Bootstrap Protocol
CD ..... Compact Disc
CDFS ..... Compact Disc File System

CHAP ..... Challenge Handshake Authentication Protocol
CIDR ..... Classless Inter-Domain Routing
CIFS ..... Common Internet File System
CMAK ..... Connection Manager Administration Kit
CNG ..... Cryptography Next Generation
COM ..... Component Object Model
CSC ..... Client-side Cache
Ctrl ..... Control
D3D ..... Direct 3D(imensional)
DACL ..... Discretionary Access Control List
DAD ..... Duplicate Address Detection
DAS ..... Direct Attached Storage
DAV ..... Datenausführungsverhinderung
DB ..... Database
DC ..... Domain Controller
DCOM ..... Distributed Component Object Model
DDC ..... Display Data Channel
DDF ..... Data Decryption Field
DDNS ..... Dynamic Domain Name System
DDoS ..... Distributed Denial of Service
Del ..... Delete
DEP ..... Data Execution Prevention
DES ..... Data Encryption Standard
DFS ..... Distributed File System
DHCP ..... Dynamic Host Configuration Protocol
DISM ..... Deployment Image Servicing and Management
DLL ..... Dynamic Link Library
DMA ..... Direct Memory Access
DNS ..... Domain Name System
DoS ..... Denial of Service
DPS ..... Diagnosis Policy Service
DRA ..... Data Recovery Agent
DRF ..... Data Recovery Field
DRM ..... Digital Rights Management
DS ..... Directory Services
DSN ..... Data Source Name
DTC ..... Distributed Transaction Coordinator
DUID ..... DHCPv6 Unique Identifier
DVD ..... Digital Versatile Disc
DWORD ..... Double word
E/A ..... Eingabe/Ausgabe
EAP ..... Extensible Authentication Protocol

EFI ..... Extensible Firmware Interface
EFS ..... Encrypting File System
Einfg ..... Einfügen
EMD ..... External Memory Device
EMS ..... Emergency Management Services
Enum ..... Enumeration
Env ..... Environment
eSATA ..... External Serial Advanced Technology Attachment
Esc ..... Escape
ESP ..... Encapsulating Security Payload
EUI ..... Extended Unique Identifier
exFAT ..... Extended File Allocation Table
FAT ..... File Allocation Table
FEK ..... File Encryption Key
Fn ..... Funktion (engl.: Function)
Fps ..... Frames per second
FQDN ..... Fully Qualified Domain Name
FTP ..... File Transfer Protocol
FVE ..... Full Volume Encryption
GB ..... Gigabyte
Gbps ..... Gigabits pro Sekunde
GC ..... Global Catalog
GDI ..... Graphic Device Interface
GPMC ..... Group-Policy Management Console
GPT ..... Globally Unique Identifier Partition Table
GRE ..... Generic Routing Encapsulation
GUI ..... Graphical User Interface
GUID ..... Globally Unique Identifier
HAL ..... Hardware Abstraction Layer
HD-DVD ..... High-Definition Digital Versatile Disc
HID ..... Human Interface Device
HKCC ..... HKEY_CURRENT_CONFIG
HKCR ..... HKEY_CLASSES_ROOT
HKCU ..... HKEY_CURRENT_USER
HKDD ..... HKEY_DYN_DATA
HKLM ..... HKEY_LOCAL_MACHINE
HKPD ..... HKEY_PERFORMANCE_DATA
HKU ..... HKEY_USERS
HRA ..... Health Registration Authority
HTML ..... Hypertext Markup Language
HTTP ..... Hypertext Transport Protocol
HW ..... Hardware

I/O ..... Input/Output
IAS ..... Internet Authentication Server
ICMP ..... Internet Control Message Protocol
ID ..... Identification
IE ..... Internet Explorer
IEEE ..... Institute of Electrical and Electronics Engineers
IGMP ..... Internet Group Management Protocol
IIS ..... Internet Information Server
IKE ..... Internet Key Exchange
Ins ..... Insert
IP ..... Internet Protocol
IPC ..... Inter-Process Communication
IPP ..... Internet Printing Protocol
IPsec ..... Internet Protocol Security
IPv4 ..... Internet Protocol Version 4
IPv6 ..... Internet Protocol Version 6
iQN ..... iSCSI Qualified Name
ISA ..... Internet Security and Acceleration
ISATAP ..... Intra-Site Automatic Tunnel Addressing Protocol
iSCSI ..... Internet Small Computer System Interface
iSNS ..... Internet Storage Name Service
IT ..... Informationstechnologie
IUSR(S) ..... Internet User(s)
Kap. ..... Kapitel
KB ..... Kilobyte
kbps ..... Kilobits pro Sekunde
KMDF ..... Kernel-Mode Driver Framework
KMS ..... Key Management Service
KTM ..... Kernel Transaction Manager
L2TP ..... Layer 2 Tunneling Protocol
LAN ..... Local Area Network
Lanman ..... LAN Manager
LCP ..... Link Control Protocol
LDS ..... Lightweight Directory Services
LIP ..... Language Interface Pack
LLMNR ..... Link-Local Multicast Name Resolution
LLTD ..... Link-Layer Topology Discovery
LLTP ..... Link-Layer Topology Protocol
LM ..... LAN Manager
LPC ..... Local Procedure Code
LPD ..... Line Printer Daemon
LPR ..... Line Printer Remote

LSA ..... Local Security Authority
LUN ..... Logical Unit Number
MAC ..... Mandatory Access Control, Medium/-a Access Control
MAK ..... Multiple Activation Key
MB ..... Megabyte
Mbps ..... Megabits pro Sekunde
MBR ..... Master Boot Record
MCITP ..... Microsoft Certified IT Professional
MCP ..... Microsoft Certified Professional
MCTS ..... Microsoft Certified Technology Specialist
MCX ..... Media Center Extender
MD4 ..... Message Digest 4
MD5 ..... Message Digest 5
mDNS ..... Multicast Domain Name System
MFT ..... Master File Table
MIC ..... Mandatory Integrity Control
MLD ..... Multicast Listener Discovery
MMC ..... Microsoft Management Console
MMU ..... Memory Management Unit
MPPE ..... Microsoft Point-to-Point Encryption
MS-CHAP ..... Microsoft-CHAP
MS-CHAPv1 ..... Microsoft-CHAP Version 1
MS-CHAPv2 ..... Microsoft-CHAP Version 2
MSDTC ..... Microsoft Distributed Transaction Coordinator
MSIE ..... Microsoft Internet Explorer
MSMQ ..... Microsoft Message Queuing
MTU ..... Maximum Transmission Unit
MU ..... Microsoft Update
MUI ..... Multilingual User Interface
MVK ..... Microsoft Verwaltungskonsole
N/V ..... Nicht verfügbar
NAP ..... Network Access Protection
NAS ..... Network Attached Storage
NAT ..... Network Address Translation
NAPT ..... Network Address/Port Translation
NAT-PT ..... Network Address Translation-Protocol Translation
NAT-T ..... Network Address Translation-Traversal
ND ..... Neighbor Discovery
Net ..... Network
NetBEUI ..... NetBIOS Extended User Interface
NetBIOS ..... Network Basic Input/Output System
NetBT ..... NetBIOS over TCP/IP

NFS ..... Network File System
NLA ..... Network Location Awareness
NRPT ..... Name Resolution Policy Table
NT ..... New Technology
NTP ..... Network Time Protocol
NTFS ..... New Technology File System
NTLM ..... New Technology LAN Manager
NTLMv2 ..... New Technology LAN Manager Version 2
NTOS ..... New Technology Operation System
NTP ..... Network Time Protocol
Num ..... Numerisch/Numeric
NUMA ..... Non-Uniform Memory Access
NVRAM ..... Non-Volatile Random Access Memory
NWLink ..... NetWare-Link
NX ..... No Execute
ODBC ..... Open Database Connectivity
OLE ..... Object-Linking and Embedding
OLE-DB ..... Object-Linking and Embedding for DataBases
OOBE ..... Out-of-Box Experience
OS ..... Operating System
P2P ..... Peer-to-Peer
PAE ..... Physical Address Extensions
PAP ..... Password Authentication Protocol
PAT ..... Port Address Translation
PATA ..... Parallel Advanced Technology Attachment
PC ..... Personal Computer
PCA ..... Program Compatibility Assistant
PCI ..... Peripheral Component Interconnect
PCI-X ..... Peripheral Component Interconnect Extended
PCIe ..... Peripheral Component Interconnect Express
PCR ..... Platform Configuration Register
PDA ..... Personal Digital Assistant
PDC ..... Primary Domain Controller
PDH ..... Performance Data Helper
PEAP ..... Protected Extensible Authentication Protocol
PIN ..... Personal Identification Number
Ping ..... Packet InterNet Groper
PnP ..... Plug and Play
PMP ..... Protected Media Path
PNRP ..... Peer Name Resolution Protocol
Pos1 ..... Position 1
POSIX ..... Portable Operating System Interface for Unix

POST ..... Power-On Self-Test
PPP ..... Point-to-Point-Protocol
PPTP ..... Point-to-Point Tunneling Protocol
PTE ..... Page Table Entry/-ies
PTR ..... Pointer
PUMA ..... Protected User Mode Audio
PVP ..... Protected Video Path
RSA ..... Rivest, Shamir, Adleman
PXE ..... Preboot Execution Environment
QoS ..... Quality of Service
RA ..... Router Advertisement
RAC ..... Reliability Analysis Component
RADIUS ..... Remote Authentication Dial In User Service
RAID ..... Redundant Array of Inexpensive Disk-Drives
RAM ..... Random Access Memory
RAS ..... Remote Access Service
RC4 ..... Rivest Cipher 4
RDC ..... Remote Differential Compression
RDP ..... Remote Desktop Protocol
RFC ..... Request for Comments
RFM ..... Reduced Functionality Mode
RID ..... Relative ID
RIP ..... Router Information Protocol
RM ..... Remote Management
RODC ..... Read-Only Domain Controller
ROM ..... Read-Only Memory
RPC ..... Remote Procedure Call
RRAS ..... Routing and Remote Access Service
RS ..... Router Solicitation
RSAT ..... Remote Server Administration Tools
RTM ..... Release to Manufacturing
SACL ..... System Access Control List
SAM ..... Security Accounts Manager
SAN ..... Storage Area Network
SAS ..... Serial Attached Small Computer Systems Interface
SATA ..... Serial Advanced Technology Attachment
SCCM ..... System Center Configuration Manager
SCM ..... Service Control Manager
SCSI ..... Small Computer Systems Interface
SD ..... Secure Digital, System Deployment
SFU ..... Services for Unix
SHA ..... Secure Hash Algorithm

SID ..... Security Identifier
SIM ..... System Image Manager
SL ..... Software License
SMB ..... Server Message Blocks
SMB2 ..... Server Message Blocks Version 2
SNMP ..... Simple Network Management Protocol
SOHO ..... Small Office or Home Office
SP ..... Service Pack
SPAP ..... Secure Password Authentication Protocol
SPN ..... Service Principal Name
SQL ..... Structured Query Language
Srv ..... Server/Service
SSD ..... Solid State Disk
SSDP ..... Simple Service Discovery Protocol
SSID ..... Service Set Identification
SSL ..... Secure Sockets Layer
SSO ..... Single Sign-On
SSTP ..... Secure Socket Tunneling Protocol
Strg ..... Steuerung
SUA ..... Subsystem für Unix-basierte Anwendungen
Svc ..... Service
SW ..... Software
SZSL ..... Systemzugriffssteuerungsliste
Tab ..... Tabulator
TAPI ..... Telephony Application Programming Interface
TB ..... Terabyte
TCP ..... Transmission Control Protocol
TCP/IP ..... Transmission Control Protocol/Internet Protocol
TFAT ..... Transaction-Safe File Allocation Table
TFTP ..... Trivial File Transfer Protocol
TIFF ..... Tagged Image File Format
TLS ..... Transport Layer Security
TPM ..... Trusted Platform Module
TS ..... Terminal Services
TSCS ..... Terminal Services Configuration Service
UAC ..... User Account Control
UDF ..... Universal Disk Format
UDP ..... User Datagram Protocol
UEFI ..... Unified Extensible Firmware Interface
UI ..... User Interface
UMDF ..... User-Mode Driver Framework
UNC ..... Universal Naming Convention

UPN ..... User Principal Name
UPnP ..... Universal Plug-and-Play
URI ..... Uniform Resource Identifier
URL ..... Uniform Resource Locator
USB ..... Universal Serial Bus
USMT ..... User-State Migration Protocol
UUCP ..... User to User Copy
VAMT ..... Volume Activation Management Tool
VB ..... Visual Beginner's All-purpose Symbolic Instruction Code
VFAT ..... Virtual File Allocation Tables
VHD ..... Virtual Harddisk
VMK ..... Volume Master Key
VMM ..... Virtual Memory Manager
VoIP ..... Voice over IP
VPN ..... Virtual Private Network
VSS ..... Volume Shadow Copy Service
WAIK ..... Windows Automated Installation Kit
WAN ..... Wide Area Network
WAS ..... Windows Activation Services
WDDM ..... Windows Display Driver Model
WDF ..... Windows Driver Framework
WDS ..... Windows Deployment Services
WebDAV ..... Web-based Distributed Authoring and Versioning
WEI ..... Windows Experience Index
WEP ..... Wired Equivalent Privacy
WER ..... Windows Error Reporting
WIM ..... Windows Imaging Format
WIMFS ..... Windows Imaging Format File System
WINS ..... Windows Internet Name Service
WinPE ..... Windows Preinstallation Environment
WinSAT ..... Windows System Assessment Tool
WLAN ..... Wireless Local Area Network
WMI ..... Windows Management Instrumentarium
WMP ..... Windows Media Player
WOW32 ..... Windows-on-Windows 32
WOW64 ..... Windows-on-Windows 64
WPA ..... Wi-Fi Protected Access
WPAD ..... Web Proxy Autodiscovery Protocol
WPF ..... Windows Presentation Foundation
WSC ..... Windows Security Center
WSS ..... Windows SharePoint Services

WSUS ..... Windows Server Update Services
WU ..... Windows Update
WWW ..... World Wide Web
WZSL ..... Wahlfreie Zugriffssteuerungsliste
XD ..... Execute Disable
XML ..... Extended Markup Language
XOR ..... Exclusive Or
XP ..... Experience
XPS ..... XML Paper Specification
ZSE ..... Zugriffssteuerungseintrag
ZSL ..... Zugriffssteuerungsliste

1. Die Systemarchitektur von Windows 7

Windows 7 ist die siebte und damit gegenwärtig neueste Version der Windows-Betriebssystem-Familie. Über die „7“ im Namen gab es viele Spekulationen: Ist die „7“ eine Anlehnung an den Nachnamen von Bill Gates als einem der drei Microsoft-Gründern? Schließlich ist das „G“ der siebte Buchstabe im Alphabet. Wie sonst kommt Microsoft auf die Vorstellung, dass sie erst jetzt, nach all den 1.x, 2.x, 3.x, 9x etc. Versionen ausgerechnet die siebte Windows-Version veröffentlichen?

Microsoft erklärt es in einem Blog-Eintrag[1] so: 1.0 ⇨ 2.0 ⇨ 3.x ⇨ 95/98/ME (9x) (4.0) ⇨ XP ⇨ Vista ⇨ Windows 7.

Einer solchen Auffassung kann der Autor dieses Buchs nicht folgen. Windows 7 ist schließlich kein „DOS-Aufsatz“, sondern steht in der Reihe der NT-Betriebssystem-Familie. Und unter dieser Betrachtungsweise ist Windows 7 tatsächlich die siebte Version von NT: NT 3.1 (allererste Version) ⇨ NT 3.5x ⇨ NT 4.0 ⇨ Windows 2000 ⇨ Windows XP ⇨ Windows Vista ⇨ Windows 7.

Intern trägt Windows 7 jedoch die Versionsnummer 6.1. Ein wichtiger Grund dafür liegt in der Kompatibilität mit anderer Software: Viele Programme prüfen anhand der Versionshauptnummer die Ausgabe des vorliegenden Betriebssystems ab. Und da besteht die Gefahr, dass auch ältere, für Windows Vista geschriebene Programme mit einer Versionsnummer „7“ nichts anfangen können und z. B. auf einer „6“ bestehen (für Vista), obwohl Windows 7 voll mit Windows Vista kompatibel ist. Das heißt, praktisch alle Programme, die unter Windows Vista lauffähig sind, funktionieren auch ohne Änderungen unter Windows 7.

Die Windows-NT-Betriebssystem-Familie zeichnet sich durch hohe Stabilität und Sicherheit aus. Microsoft verspricht sogar, mit Windows 7 die robusteste und sicherste Windowsversion ausgeliefert zu haben. Aber wie wird dies realisiert?

Das Betriebssystem Windows 7 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] http://windowsteamblog.com/blogs/windowsvista/archive/2008/10.aspx

M. Grotegut, *Windows 7*, X.systems.press, DOI 10.1007/978-3-642-01035-4_1,

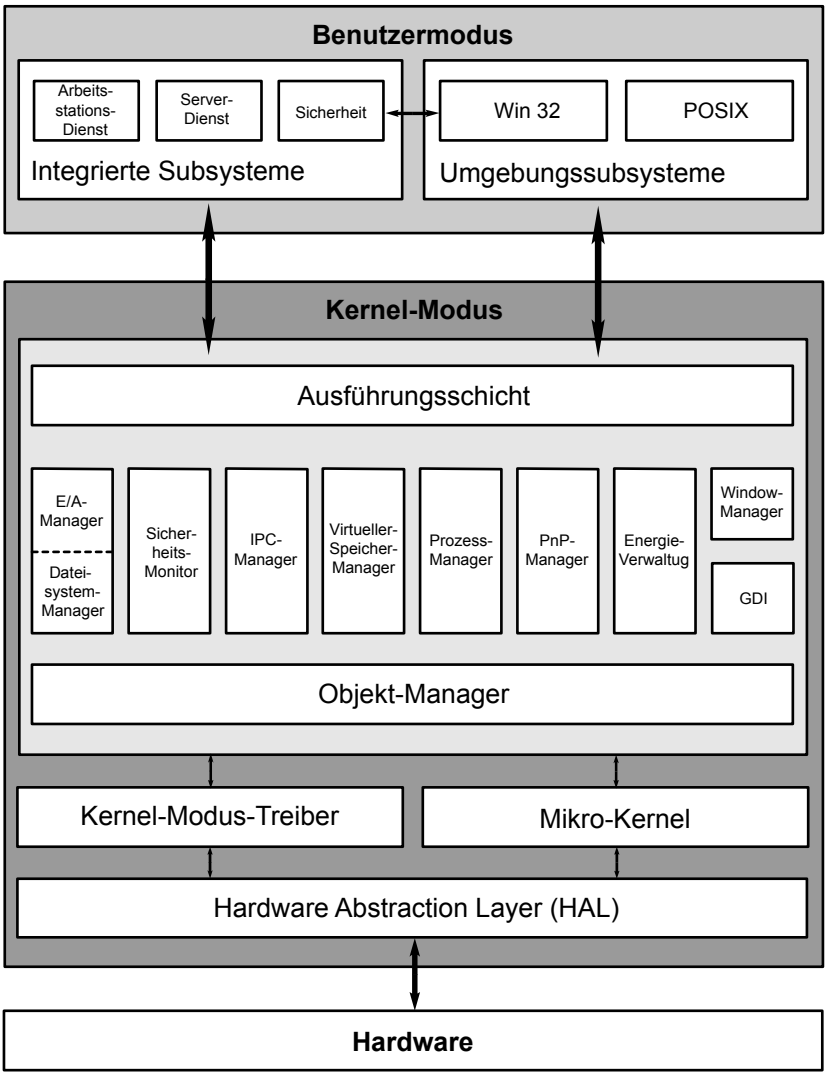

Abb. 1.1. Windows 7 Systemarchitektur

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.[2] 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), die um einen Mikro-Kernel herum realisiert, und z. T. in einzelnen Dateien enthalten sind, und ist daher nicht *monolithisch*. Andererseits hat der Windows-7-Kernel aber auch nicht eine Mikro-Kernel-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

Durch die HAL (Hardware Abstraction Layer) werden sämtliche Geräte und Schnittstellen im System virtualisiert und hardwareabhängige Details wie Interruptcontroller, E/A-Schnittstellen etc. verborgen. 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 geringfügig 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 dieser genannten Funktionen sind in der Datei HAL.DLL enthalten.

[2] So ist z. B. die Virtualisierung der Benutzerkontensteuerung im Kernel realisiert.

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, Kernel Transactionmanager- (Ktm) und Interruptweiterleitungsfunktionen.

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

1.1.3 Der Scheduler

Ein Bestandteil des Mikro-Kernels ist der *Scheduler*. Er steuert die Zuordnung und Länge der zur Ausführung bereiten einzelnen Threads auf die zur Verfügung stehenden CPUs bzw. -Kerne. Dadurch wird entschieden, welche Threads ausgeführt werden sollen und wie lange sie jeweils CPU-Zeit erhalten. Er kann in den 32-Bit-Varianten bis zu 32, und in den 64-Bit-Varianten bis zu 256 CPUs (bzw. CPU-Kerne) gleichzeitig mit Threads belegen.

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 Anwender weiß, auf welcher Seite er sich befindet, die Rechtschreibkorrektur, die Grammatikprüfung usw. aus.

1.1.4 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.[3]

[3] Bei einer digitalen Signatur wird über einen Text- oder Code-Block ein Hash-Verfahren wie MD5 oder SHA-1 angewendet, das einen kurzen „Fingerabdruck“ (z. B. 160 Bits) erzeugt und diesen mit dem privaten Schlüssel eines asymmetrischen Verschlüsselungsalgorithmus codiert. Eine Prüfung kann dadurch erfolgen, dass auf einem System der gleiche Hashalgorithmus auf denselben Datenblock angewendet wird und das Ergebnis mit dem durch Entschlüsselung mit dem bekannten öffentlichen Schlüssel erhaltenen Original Hash-Wert verglichen wird: Wenn nur ein einziges Bit der Daten absichtlich oder unab-

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

Die Treibersignatur ist für die 64-Bit-Varianten von Windows 7 obligatorisch (siehe unten)[4]. Für die 32-Bit-Varianten ist sie zwar freigestellt, es bringt aber dennoch Vorteile mit sich, wenn Treiber signiert sind, denn neben dem Schutz gegen Kernel-Viren und -Trojaner müssen für die Wiedergabe von hochaufgelösten (engl.: High Definition, HD) Inhalten alle Kernel-Modus-Treiber auch in den 32-Bit-Version digital signiert sein![5]

1.1.5 Die Ausführungsschicht

Die Ausführungsschicht (engl.: Executive) ist ein Bindeglied zwischen den Benutzermodus-Subsystemen und den anderen Kernel-Bestandteilen und ist damit ein Hauptbestandteil des Windows-7-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*.[6]

1.1.6 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 7 objektorientiert zu sein und der Zugriff hierauf wird durch Klassen und Methoden realisiert.

Andere wichtige Aufgaben des Objektmanagers sind, den gleichzeitigen Zugriff auf Systemressourcen zu steuern, so dass es hierbei nicht zu Kon-

---

sichtlich (bsp. durch Übertragungsfehler) geändert ist, sind die beiden Hash-Werte ungleich und die Änderung wird erkannt.

[4] Keine Regel ohne Ausnahme: Es gibt einen Schalter der Startumgebung, mit dem diese Prüfung abgeschaltet werden kann (siehe Anhang).

[5] Siehe dazu Kapitel 1.4.

[6] 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.

flikten kommt, und den Speicher für Objektbeschreibungsstrukturen anzufordern und freizugeben.

1.1.7 Der E/A-Manager

Der Eingabe-/Ausgabe-Manager (engl.: Input/Output-Manager bzw. I/O-Manager) steuert die Kommunikation zwischen den Benutzermodus-Subsystemen und den Kernel-Modus-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.

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

Der E/A-Manager arbeitet eng mit dem 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 überhaupt verwendet werden.