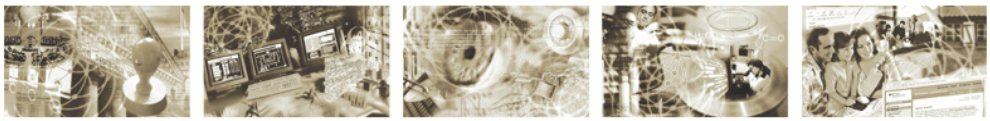
Bundesamt
für Sicherheit in der
Informationstechnik



Anleitung zur Installation und Minimierung eines Arbeitsplatz-PCs mit Windows 7

BSI-Standards zur Internet-Sicherheit

Version 1.01

Vervielfältigung und Verbreitung

Dies ist ein Werk der ISi-Reihe. Ein vollständiges Verzeichnis der erschienenen Bände finden Sie auf den Internet-Seiten des BSI.

http://www.bsi.bund.de oder http://www.isi-reihe.de

Bundesamt für Sicherheit in der Informationstechnik
ISi-Projektgruppe
Postfach 20 03 63
53133 Bonn
Tel. +49 (0) 228 99 9582-0
E-Mail: isi@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Beim vorliegenden Dokument handelt es sich um eine Anleitung zur Installation und Konfiguration von Windows 7 auf einem APC, wie er typischerweise für Bürotätigkeiten verwendet wird. Es wird nur die Absicherung des Betriebssystems betrachtet. Die Absicherung von Anwendungen wie Browser oder E-Mail-Client und weitere Komponenten wie Virenschutzprogramm und Gerätekontrolle, sind nicht Teil dieses Dokuments. Informationen zu diesen Themen finden sich in den Studien *Absicherung eines PC-Clients* [ISi-Client], *Sichere Nutzung von Web-Angeboten* [ISi-Web-Client] und *Sichere Nutzung von E-Mail* [ISi-Mail-Client].

1.1 Zielsetzung und Zielgruppe

Dieses Dokument erläutert Schritt für Schritt, wie Windows 7 auf einem APC installiert und konfiguriert werden kann. Die Zielgruppe dieser Anleitung sind daher in erster Linie Administratoren.

Zielsetzung ist es, das Betriebssystem möglichst sicher zu konfigurieren und weiterhin die Funktionsfähigkeit des APCs zu gewährleisten.

Als Referenzsystem wird ein typischer Büro-APC betrachtet. Dieser zeichnet sich durch folgende Eigenschaften aus: Der APC

- befindet sich im internen Netz hinter einem Sicherheits-Gateway (siehe auch [ISi-LANA])
- ist Bestandteil einer Windows-Domäne
- wird zentral administriert
- wird von einem Benutzer verwendet (kein Mehrbenutzersystem)
- wird für Bürotätigkeiten verwendet

Da es sich um einen APC für Bürotätigkeiten handelt, sind neben dem Betriebssystem noch folgende Anwendungen vorgesehen:

- Office-Paket (Textverarbeitung, Tabellenkalkulation, Präsentationserstellung)
- PDF-Viewer (Adobe Reader X)
- Internet-Browser (Microsoft Internet-Explorer und Alternativprodukte wie z. B. Google Chrome oder Mozilla Firefox)
- E-Mail- und Kalender-Programm
- Programm zur Medienwiedergabe (Windows Media Player)

1.2 Aufbau des Dokuments

Das Dokument ist folgendermaßen aufgebaut:

- Abschnitt 2 erläutert die notwendigen Grundlagen und Werkzeuge zur Konfiguration.
- Abschnitt 3 geht kurz auf die Installation des Basissystems ein.
- Abschnitt 4 beschreibt Schritt für Schritt, wie Windows 7 nach der Installation sicher zu konfigurieren ist.
- Abschnitt 5 betrachtet abschließend die Erstellung und Verteilung eines Referenzsystems.

2 Grundlagen

Dieser Abschnitt geht auf einige Eigenschaften von Windows 7 ein und beschreibt die wesentlichen Werkzeuge, die bei der Konfiguration in Abschnitt 4 verwendet werden. Allgemeine Informationen zu APCs und Betriebssystemen finden sich in [ISi-Client].

2.1 Informationen zu Windows 7

Das Betriebssystem Windows 7 ist eine Software, die als Basis für die Installation und die Nutzung von Anwendungen dient. Betriebssysteme für Client-PCs bestehen in der Regel aus mehreren Komponenten, wie dem Betriebsystem-Kern (Kernel), einer Benutzeroberfläche sowie Konfigurations- und Anwendungsprogrammen. Der Betriebssystem-Kern wird nach dem Einschalten des PCs vom BIOS/EFI geladen und gestartet. Zu seinen wesentlichen Aufgaben gehören:

- die Ausführung von Programmen,
- die Verteilung und Verwaltung von Betriebsmitteln,
- die Steuerung der Ein- und Ausgabegeräte,
- die Bereitstellung von Schnittstellen zum Zugriff auf die Hardware sowie
- die Kontrolle der Benutzerrechte.

Neben dem Kernel-Modus existiert zusätzlich ein Anwender- oder Benutzermodus (User-Mode). In diesem Modus können Anwendungsprogramme ausgeführt werden. Da der Kernel-Mode die Abstraktion von Betriebssystem und Hardware darstellt, besitzt dieser Modus einen höheren, privilegierteren Status als der User-Mode.

Der Zugriff auf die Hardware erfolgt über Gerätetreiber. Typischerweise bringen Betriebssysteme bereits eine ganze Reihe von Treibern für verschiedene Geräte, wie beispielsweise Grafikkarten oder USB-Geräten[1], mit. Der Einsatz spezieller Hardware erfordert häufig die nachträgliche Installation weiterer Treiber, die in der Regel vom Hardware-Hersteller bereitgestellt werden[2].

Das Betriebssystem steuert auch die Ein- und Ausgabegeräte, über die der Benutzer mit dem Betriebssystem interagiert. Um diese Interaktion zu vereinfachen, stellen Betriebssysteme dem Benutzer eine sogenannte Benutzeroberfläche zur Verfügung. Dabei kann es sich um eine textbasierte (Komandozeileninterpreter, Shell) oder eine grafische Oberfläche (GUI) handeln.

Anwendungsprogramme kommunizieren direkt mit dem Betriebssystem. Dazu stellt das Betriebssystem Schnittstellen in Form von Bibliotheken bereit, um Anwendungen beispielsweise den Zugriff auf die Hardware zu ermöglichen. Die Verwaltung der verfügbaren Betriebsmittel, wie Arbeitsspeicher und Prozessor-Rechenzeit, erfolgt durch das Betriebssystem.

2.1.1 Windows 7 Versionen

Windows 7 ist in mehreren Versionen verfügbar, die sich im Funktionsumfang unterscheiden. Die Versionen *Starter, Home Basic, Home Premium* richten sich an Privatanwender und *Ultimate* an fortgeschrittene Anwender, wohingegen die Versionen *Professional* und *Enterprise* Unternehmenskunden adressieren. Tabelle 1[3] listet einige im Kontext dieses Dokumentes wichtige Funktionen und die Unterstützung durch die unterschiedlichen Betriebssystemversionen auf.

1 Die Absicherung von Hardware-Schnittstellen ist nicht Bestandteil dieses Dokumentes. Siehe hierzu [ISi-Client].
2 Unter Windows 7 mit 64-bit müssen diese Treiber signiert sein.
3 http://windows.microsoft.com/de-de/windows7/products/compare

Funktionen	*Windows 7 Starter*	*Windows 7 Home Basic*	*Windows 7 Home Premium*	*Windows 7 Professional*	*Windows 7 Ultimate*	*Windows 7 Enterprise*
Media-Center		X	X	X	X	
XP-Modus				X	X	X
Domänenbeitritt				X	X	X
BitLocker					X	X
Sicherung über LAN				X	X	X
Remote Desktop Host				X	X	X
AppLocker					X	X
Direct Access					X	X
Bootvorgang von virtuellen Festplatten					X	X
Verschlüsseltes Dateisystem				X	X	X
Heimnetzgruppe	Nur Beitritt	Nur Beitritt	X	X	X	X
Schneller Benutzer-Wechsel		X	X	X	X	X

Tabelle 1: Unterschiede beim Funktionsumfang verschiedener Windows 7 Versionen

2.1.2 Upgrade

Ist bereits Windows Vista installiert, so kann dieses auf Windows 7 upgegradet werden. Tabelle 2 stellt dar, welche Vista Version auf welche Windows 7 Version upgegradet werden kann. Ein Wechsel von 32- zu 64-bit oder umgekehrt ist nicht möglich.

Upgrade Richtung →	*Windows 7 Starter*	*Windows 7 Home Basic*	*Windows 7 Home Premium*	*Windows 7 Professional*	*Windows 7 Ultimate*	*Windows 7 Enterprise*
Vista Home Basic			X			
Vista Home Premium			X		X	
Vista Business				X	X	
Vista Ultimate					X	
XP						

Tabelle 2: Mögliche Upgrades von Windows Vista auf Windows 7

2.1.3 Lizenzmodell

Es werden unterschiedliche Lizenzmodelle von Microsoft angeboten:

- Original-Equipment-Manufacturer (OEM): Die Software (Betriebssystem oder Office-Produkt) ist an eine Hardware bzw. einen PC lizenzrechtlich gebunden ist und kann nur in Verbindung mit dieser spezifischen Hardware genutzt werden. In der Regel besteht keine Möglichkeit eines Upgrade auf eine höhere Windows-Version.

- Einzelplatzlizenz: Sie ist wie die OEM Version an einen PC gebunden und kann allerdings nachträglich lizenziert werden, während die OEM nur mit einer Hardware erworben werden kann. Es besteht weiterhin die Möglichkeit, ein Upgrade der Lizenzen auf eine nächst höhere Windows-Version durchzuführen.
- Volumenlizenzprogramm: Dieses Lizenzmodell wird in Unternehmen bzw. Firmen und Organisationen eingesetzt, die mehr als fünf PCs im Einsatz haben. Lizenzen sind damit nicht an einer Hardware oder einem PC gebunden. Dabei wird das Lizenzmodell in vier Kategorien eingeteilt.
  - Volumenlizenz *Open License*: Durch eine einmalige Zahlung erwirbt der Käufer eine entsprechende Anzahl von Lizenzen. Dabei kann man erworbene OEM Versionen über eine zusätzliche vertraglichen Regelung (Microsoft Software Assurance) in das Volumenlizenzprogramm überführen. Dies schließt die entsprechenden Nutzungsrechte, kostenlose Upgrades sowie Support ein.
  - Volumenlizenz *Open Value*: Mit dieser Variante wird über einen bestimmten Zeitraum (meist drei Jahre) ein Mietvertrag für genutzte Lizenzen abgeschlossen. Während dieser Vertragslaufzeit kann ein bestehendes Kontingent von initialen Lizenzen frei genutzt werden ohne eine Bindung an einem bestimmten PC. Dieses Modell beinhaltet die Microsoft Software Assurance.
  - Volumenlizenz *Microsoft Open Value Company-Wide*: Mit diesem Modell können Unternehmen ihre Lizenzen standort- und unternehmensweit standardisieren und damit einfacher verwalten. Dieses Modell beinhaltet die Microsoft Software Assurance.
  - Volumenlizenz *Open Value Subscription*: Dieses Modell ermöglicht eine genaue Kostenplanung im Lizenzbereich. Zu Beginn eines Vertragsjahrs wird die Anzahl der zu lizenzierenden PCs festgelegt. Diese Anzahl kann dem tatsächlichen Bedarf entsprechend variabel angepasst werden. Dieses Modell beinhaltet die Microsoft Software Assurance.

Tabelle 3 stellt die verschiedenen Windows-Versionen den verfügbaren Lizenzmodellen gegenüber. Dabei ist zu erkennen, dass die Version Windows 7 Enterprise mit ihrem Volumenlizenzprogramm speziell auf Unternehmen ausgerichtet ist. Windows 7 Professional kann im Gegensatz zu seinen Vorgängerversionen mit einer aktiven Microsoft Software Assurance auf die Windows 7 Enterprise angehoben werden. Die Windows 7 Ultimate ist vom Funktionsumfang her betrachtet die höchste Lizenz außerhalb des Volumenlizenzprogramms.

Windowsversion	***Lizenzmodell***
Windows 7 Starter	OEM
Windows 7 Home Basic	OEM, Einzelplatzlizenz
Windows 7 Home Premium	OEM, Einzelplatzlizenz
Windows 7 Professional	OEM, Einzelplatzlizenz, Volumenlizenzprogramm
Windows 7 Ultimate	OEM, Einzelplatzlizenz
Windows 7 Enterprise	Volumenlizenzprogramm

Tabelle 3: Übersicht der Windows 7 Versionen Lizenzen

2.1.4 Produktaktivierung

Um Windows 7 produktiv verwenden zu dürfen, muss eine Aktivierung bei Microsoft erfolgen. Die Aktivierung ist per Internet, Modem oder Telefon möglich und kann bei der Installation oder zu einem späteren Zeitpunkt durchgeführt werden.

Des Weiteren kann ein Volumenlizenzkunde durch die Verwendung eines zentralen *Key Management Service* (KMS) und des *Software License Managers* (SL-Manager oder auch `Slmgr.vbs`) eine automatisierte und übersichtliche Aktivierung vornehmen[4]. Hierbei wird der KMS auf einem Windows 7 oder Windows 2008 R2 gestartet und dieser KMS-Host den zu aktivierenden Clients zugewiesen. Hierbei müssen diverse Registry-Schlüssel angepasst und je nach Netzwerkumgebung einige Konfigurationen oder Dienste (z. B. DNS) geändert werden.[5]

Wird der Aktivierungsprozess während der Installation übersprungen, verbleiben noch 30 Tage in denen das System aktiviert werden muss[6]. Mittels vorhandener Systemwerkzeuge[7] (`slmgr.vbs /rearm`) kann die Aktivierung manuell bis zu drei mal zurückgesetzt werden, was die Gesamtaktivierungsdauer auf bis zu 120 Tage erhöht. Hierdurch ist es in größeren Umgebungen möglich, einen Rollout und die nötige Aktivierung innerhalb von 120 Tagen vorzunehmen.

Unter Umständen kann es vorkommen, dass eine bereits aktivierte Version des verwendeten Windows 7 nochmals aktiviert werden muss. Dies ist dann der Fall, wenn sich die Hardware-Konfiguration des PCs ändert. Windows 7 vergibt während der Installation einen Grundwert für das System in Höhe von 35 Punkten, die sich auf einzelne Komponente (Grafikkarte, CPU, Speicher, Festplatte, usw.) verteilt. Beim Tausch der Komponenten werden diese Komponentenwerte vom Grundwert abgezogen. Sinkt der gesamte Punktwert unter den vom Hersteller definierten Schwellwert von 26, wird automatisch eine erneute Aktivierung gefordert, die innerhalb von drei Tagen erfolgen muss.

2.1.5 Hardwareanforderungen

Microsoft hat Systemanforderungen definiert, die die Hardware erfüllen sollte, um Windows 7 zu betreiben. Tabelle 4 fasst diese Mindestanforderungen zusammen[8].

Komponenten	*Windows 7 (32-bit)*	*Windows 7 (64-bit)*
Prozessor (CPU)	Min. 1 GHz	
Festwertspeicher (RAM)	1 GB	2 GB
Festplatte	16 GB	20 GB
Grafikkarte	Direct-X mit WDDM 1.0	
XP-Mode	Zusätzliche 1 GB RAM und 15 GB Festplattenplatz	
Windows Media Center	Zusätzliche Audio- und TV-Hardwareunterstützung	

Tabelle 4: Mindestanforderungen des Herstellers

Es sei angemerkt, dass es sich hierbei um Minimalanforderungen handelt und damit lediglich eine Installation des Betriebssystems ermöglicht wird. Es sollten grundsätzlich nur aktuelle Hardware-Komponenten verwendet werden. Auch muss die Verfügbarkeit entsprechender Treiber geprüft werden. Windows 7 32-bit unterstützt abhängig von der Version (siehe Abschnitt 2.1.7) unterschiedlich viel Arbeitsspeicher. Um eine optimale Leistung des APCs zu erzielen, sollten die

4 http://technet.microsoft.com/en-us/library/dd878528.aspx
5 http://technet.microsoft.com/en-us/library/ff793419.aspx
6 http://windows.microsoft.com/de-DE/windows7/Activating-Windows-7-frequently-asked-questions
7 http://technet.microsoft.com/en-us/library/ff793433.aspx
8 http://windows.microsoft.com/de-DE/windows7/products/system-requirements

benötigen Mindestanforderungen der verwendeten Programme ermittelt werden. Es wird empfohlen, für die Ermittlung des notwendigen Gesamt-Arbeitsspeichers die Anforderungen an den Arbeitsspeicher für die zu verwendenden Programme zu addieren. Tabelle 3 stellt Hardware-Anforderungen nach Erfahrungswerten im Bereich Office Anwendungen dar.

Komponenten	*Windows 7 (32-bit)*	*Windows 7 (64-bit)*
Prozessor (CPU)	Mehrkern-Prozessor	
Festwertspeicher (RAM)	3 GB	4 GB
Festplatte	160 GB	200 GB
Grafikkarte	Grafikkarte mit eigenem Video und Grafik RAM	
Windows Media Center	Zusätzliche Audio- und TV-Hardwareunterstützung	

Tabelle 5: Best Practices

Um herauszufinden, ob die Hardware eines bestehenden Windows-Systems für den Einsatz von Windows 7 geeignet ist, kann der sog. Upgrade Advisor[9] verwendet werden. Vor der Durchführung sollten alle Geräte (z. B. auch USB-Drucker) angeschlossen und angeschaltet sein. Nach erfolgter Prüfung wird ein entsprechender Statusbericht ausgegeben.

2.1.6 Treiber

Für den Zugriff auf die vorhandene Hardware (z. B. Grafikkarte, Netzwerkkarte) muss ein entsprechender Gerätetreiber (kurz: Treiber) installiert sein. Bei einem 64-bit-Betriebssystem müssen auch auf 64-bit-Technologie basierende Treiber verwendet werden (siehe Tabelle 6).

Um eine durchgängige Systemstabilität des Betriebssystems zu gewährleisten, können auf Windows 7 64-bit nur noch von Microsoft freigegebene und signierte Treiber installiert werden.

Betriebssystem-Architektur	*32-bit-Treiber*	*64-bit-Treiber*
32-bit	X	
64-bit		X

Tabelle 6: Unterstützung der Treiber-Versionen durch die Betriebssystem-Architektur

2.1.7 Speicherverwaltung

Die verschiedenen Windows 7 Versionen können unterschiedlich viel Speicher verwalten[10]. Tabelle 7 zeigt die Speichergrenzen der verschiedenen Versionen.

Betriebssystem-Version	*32-bit Architektur*	*64-bit-Architektur*
Windows 7 Starter	2 GB	2 GB
Windows 7 Home Basic	4 GB	8 GB
Windows 7 Home Premium	4 GB	16 GB
Windows 7 Professional	4 GB	192 GB
Windows 7 Ultimate	4 GB	192 GB
Windows 7 Enterprise	4 GB	192 GB

Tabelle 7: physische Speichergrenze

9 http://www.microsoft.com/windows/windows-7/get/upgrade-advisor.aspx
10 http://msdn.microsoft.com/en-us/library/aa366778(v=vs.85).aspx#physical_memory_limits_windows_7

Zusätzlich zum physischen Speicher existiert ein virtueller Adressraum[11] (Virtual Address Space), der den physischen Speicher erweitert. Der virtuelle Speicher ist in Seiten aufgeteilt, die entweder auf physische Seiten oder auf eine Auslagerungsdatei (`Pagefile.sys`) verweisen. Seiten, die lange nicht bearbeitet wurden, werden in die Auslagerungsdatei verschoben und referenziert. Der virtuelle Adressraum stellt zudem sicher, dass unterschiedliche Prozesse untereinander keinen Zugriff erhalten.

Für 32-bit Anwendungen, die unter Windows 7 64-bit ausgeführt werden, besteht die Möglichkeit 4 GB virtuellen Adressbereich zu reservieren. In Tabelle 8 sind die notwendigen Einstellungen dargestellt. Detaillierte Speicher und Adressbereich Limitierungen sind unter http://msdn.microsoft.com/en-us/library/aa366778.aspx einzusehen.

Betriebssystem-Architektur	*Virtueller Adressbereich Standardwert*	*Virtueller Adressbereich Maximalwert*[12]
32-bit Anwendung auf einem 32-bit Betriebssystem	2 GB	3 GB
32-bit Anwendung auf einem 64-bit Betriebssystem	2 GB	4 GB
64-bit Anwendung auf einem 64-bit Betriebssystem	2 GB	8 TB

Tabelle 8: Adressbereich Speicher

2.1.8 Prozessverwaltung von 32- und 64-bit Anwendungen

Neben der Entwicklung von neuen Betriebssystemfunktionen wurde bei Windows 7 auch die Unterstützung von 64-bit-Prozessorarchitekturen weiter entwickelt. Um 32-bit Applikationen ohne entsprechende Modifizierungen unter Windows 7 64-bit ausführen zu können, wurde ein neues Subsystem entwickelt. Dieses trägt den Namen WOW64 (Windows-32-on-Windows-64) und ist in allen 64-bit Versionen implementiert. Der WOW64-Emulator läuft im User-Mode und stellt Schnittstellen zwischen der 32-bit Version der Ntdll.dll und dem Kernel bereit[13] (siehe Abbildung 2.1).

11 http://msdn.microsoft.com/en-us/library/aa366525(v=VS.85).aspx
12 http://msdn.microsoft.com/en-us/library/aa384271
13 http://msdn.microsoft.com/en-us/library/aa384274.aspx

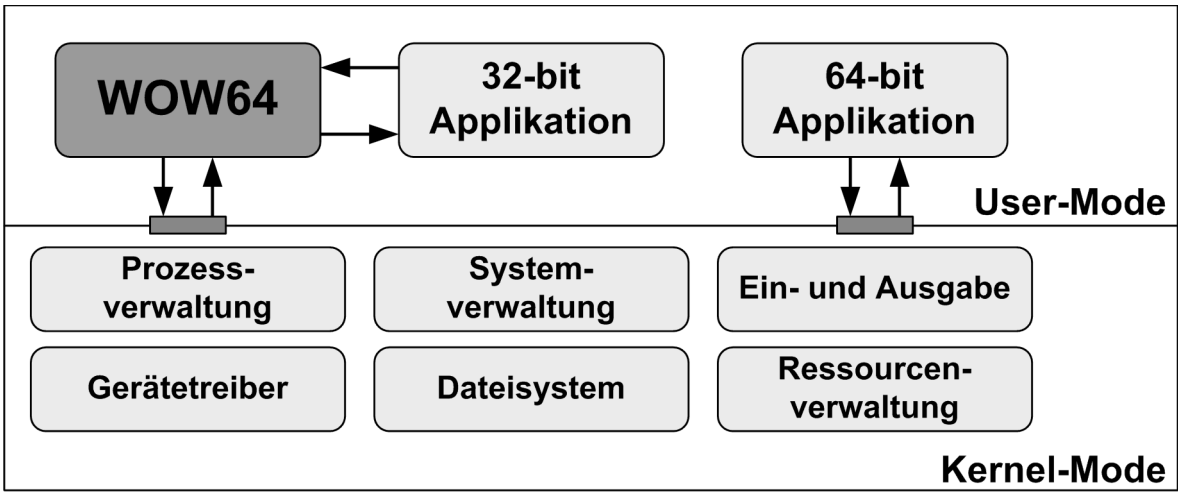


Abbildung 2.1: WOW64 Emulator bei Windows 7 mit 64-bit

Dies ist erforderlich, weil 32-bit Prozesse keine 64-bit DLLs laden können. Umgekehrt können auch 64-bit Prozesse keine 32-bit DLLs laden. Unter Windows 7 64-bit werden daher gleichnamige DLLs, Registry und Systemdateien explizit für 32-bit und für 64-bit vorgehalten.

Der WOW64 ist nur in den 64-bit Versionen von Windows 7 integriert. Auf einem 32-bit-Betriebssystem können keine 64-bit-Programme betrieben werden , da es in der Windows 32-bit Architektur keine 64-bit Unterstützung gibt. Auf einem 64-bit-Betriebssystem hingegen können durch die oben genannte WOW64 Unterstützung 32-bit-Programme betrieben werden. 16-bit-Programme werden durch den Emulator nicht mehr unterstützt (siehe Tabelle 9). Wenn 32-bit-Programme im WOW64 auf 16-bit-Programme zugreifen müssen, kommt es zu einem Fehler (`ERROR_BAD_EXE_FORMAT`)[14].

Windows-Architektur	*16-bit Programme*	*32-bit Programme*	*64-bit Programme*
32-bit	X	X	
64-bit		X	X

Tabelle 9: Unterstützung der Programme durch die Betriebssystem-Architektur

In Tabelle 10 sind die Beschränkungen und verweigerte Unterstützung des WOW64-Subsystems für ältere Programme dargestellt. Müssen noch alte Programmversionen verwendet werden, so ist dies bei der Wahl der Betriebssystem-Architektur (32- oder 64-bit) zu berücksichtigen.

Programme	*Bemerkung*
16-bit Programme	die für 16-bit Betriebssysteme kompiliert wurden
Kernelmodus-Programme	die für 32-bit Betriebssysteme kompiliert wurden
16-bit Installationsprogramme	die 32-bit Programme als Installationsroutine benötigen
32-bit Programme	die 16-bit Komponenten und deren Funktionen nutzen

Tabelle 10: Beschränkungen des WOW64-Subsystems

2.1.9 Dateiverwaltung

Mit Windows 7 hat sich auch die Organisation der Dateien verändert. Die Tabelle 11 zeigt eine Übersicht der Windows Unterverzeichnisse. Die Windows 7 64-bit Dateien liegen in dem Verzeichnis `%SystemRoot%\system32`. Die 32-bit Anwendungen greifen auf Bibliotheken aus dem

14 http://msdn.microsoft.com/en-us/library/aa384249(v=VS.85).aspx

Verzeichnis `%SystemRoot%\SysWOW64` zu. Da viele der 64-bit DDLs weiterhin die gleichen Namen wie Ihre 32-bit Versionen tragen, wurde eine Unterscheidung eingeführt. Damit gewährleistet wird, dass Dateien für verschiedene Architekturen nicht fälschlicherweise geladen werden, wurde der sog. File System Redirector eingeführt. Wenn eine 32-bit Anwendung erwartet, auf Dateien in dem Verzeichnis `%SystemRoot%\system32` zuzugreifen zu können, dann wird der Zugriff auf das Verzeichnis `%SystemRoot%\SysWOW64` umgeleitet[15]. In Tabelle 11 sind alle Verzeichnisse aufgeführt, die nicht nach `%windir%\SysWOW64` umgeleitet werden. Unabhängig der Versionen werden standardmäßig Windows Updates unter `%SystemRoot %\SofwareDistribution\Download` abgelegt. Das Verzeichnis `%SystemRoot%\winsxs` dient dazu, verschiedene Programme und DLL Versionen parallel betreiben zu können. Greifen ältere Programme auf das Standardverzeichnis `%SystemRoot%\system32` zu und sind die benötigten Dateien nicht vorhanden, dann werden diese Programme auf das Verzeichnis `%SystemRoot%\winsxs` verwiesen. Installationsprogramme legen in diesem Verzeichnis ebenfalls entsprechende Dateien ab. Dieses Verzeichnis kann sehr stark wachsen. Bei der Planung und Durchführung einer Windows 7 Installation ist dies zu beachten.

Unterverzeichnisse

`%windir%\system32\catroot`
`%windir%\system32\catroot2`
`%windir%\system32\driverstore`
`%windir%\system32\drivers\etc`
`%windir%\system32\logfiles`
`%windir%\system32\spool`

Tabelle 11: Ordnerstruktur bei Windows 7.

Prozess	***Umgebungsvariable***

32-bit	`ProgramFiles=%ProgramFiles(x86)%`
	`ProgramW6432=%ProgramFiles%`
	`CommonProgramFiles=%CommonProgramFiles(x86)%`
	`CommonProgramW6432=%CommonProgramFiles%`

64-bit	`ProgramFiles=%ProgramFiles%`
	`ProgramW6432=%ProgramFiles%`
	`CommonProgramFiles=%CommonProgramFiles%`
	`CommonProgramW6432=%CommonProgramFiles%`

Tabelle 12: Windows 7 Umgebungsvariablen[16]

2.1.10 Dynamic Link Library (DLL)

Dynamic Link Library (DLL) Dateien[17] sind Bibliotheken, die Programmcode oder Daten enthalten können, auf die mehrere Anwendungen zugreifen können. Durch das Auslagern von Programmcode in eine DLL wird Speicherplatz auf der Festplatte und im Hauptspeicher eingespart.

Viele der benötigten DLLs werden schon bei der Installation des Betriebssystems auf dem APC abgelegt. In der Regel befinden sich die DLLs im Systemverzeichnis von Windows. Der Pfad bei einem 32-bit Betriebssystem lautet: `C:\Windows\System32`. Bei einem 64-bit Betriebssystem werden die 64-bit DLLs im Pfad `C:\Windows\System32` und die 32bit DLLs im Pfad

15 http://msdn.microsoft.com/en-us/library/aa384187%28VS.85%29.aspx
16 http://msdn.microsoft.com/en-us/library/aa384274%28v=vs.85%29.aspx
17 http://support.microsoft.com/kb/815065/de

`C:\Windows\Syswow64` abgelegt[18] [19]. Software, die eigene DLLs mitinstalliert, legt diese in der Regel im Verzeichnis oder Unterverzeichnis des Programms ab.

2.2 Werkzeuge zur Verwaltung

2.2.1 Eingabeaufforderung

Die Eingabeaufforderung (engl. Command Prompt) wird für die Eingabe von MS-DOS (Microsoft Disk Operating System) Befehlen verwendet (siehe Abbildung 2.2). Durch die Verwendung der Befehlszeile kann Windows 7 auch ohne grafische Oberfläche verwaltet werden. Die Eingabeaufforderung lässt Eingabe von `CMD` in das Suchfeld des Startmenüs oder über Start → Alle Programme → Zubehör → Eingabeaufforderung aufrufen.

Eine Liste mit allen Kommandozeilenbefehlen und deren Syntax kann unter http://technet.microsoft.com/en-us/library/cc754340(v=ws.10).aspx eingesehen werden.

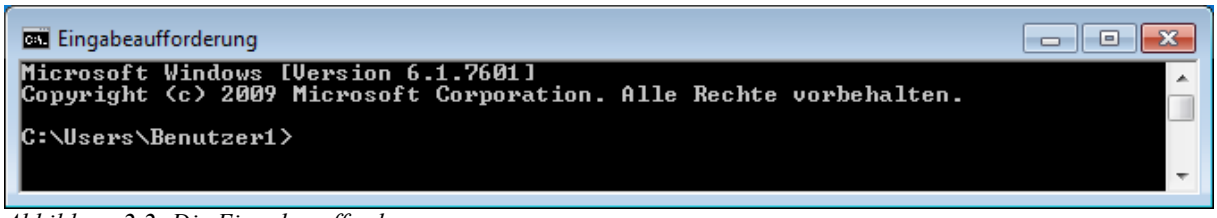


Abbildung 2.2: Die Eingabeaufforderung

2.2.2 Systemsteuerung

Die Systemsteuerung beinhaltet Anwendungen zur Steuerung und Konfiguration einer Windows 7 Umgebung. Die in der Systemsteuerung bereitgestellten Software-Komponenten können von einem Systemverantwortlichen verwendet werden[20]. Die Systemsteuerung dient u. a. zur allgemeinen Administration (z. B. Darstellung des Desktops, Hardware-Einstellungen), zur Einstellung von installierten Programmen und für sicherheitsrelevante Einstellungen (z. B. Firewall, Windows Defender).

Die Systemsteuerung kann über Start → Systemsteuerung aufgerufen werden. Abbildung 2.3 zeigt die Systemsteuerung in der klassischen Ansicht mit großen Symbolen[21].

Die Anwendungen der Systemsteuerung können ebenfalls über die Eingabeaufforderung gestartet werden. Hierzu muss der entsprechenden Name der Anwendung mit der Dateiendung `.cpl` in der Eingabeaufforderung eingegeben werden. Nachfolgender Befehl öffnet beispielsweise das Fenster zur Einstellung der lokalen Sicherheitsrichtlinien:

```
c:> wscui.cpl
```

Um die vorhandenen Applikationen der Systemsteuerung zu ermitteln, kann ebenfalls in der Eingabeaufforderung im Wurzelverzeichnis folgender rekursive Befehl abgesetzt werden[22]:

```
c:> dir *.cpl /s
```

Weitere Informationen zu CPL-Dateien können unter http://support.microsoft.com/kb/192806 nachgelesen werden.

18 http://support.microsoft.com/kb/282747
19 http://support.microsoft.com/kb/896456/de
20 http://windows.microsoft.com/de-DE/windows7/Working-with-Control-Panel
21 http://windows.microsoft.com/de-DE/windows-vista/Change-Control-Panel-to-Classic-view
22 http://support.microsoft.com/kb/149648/de

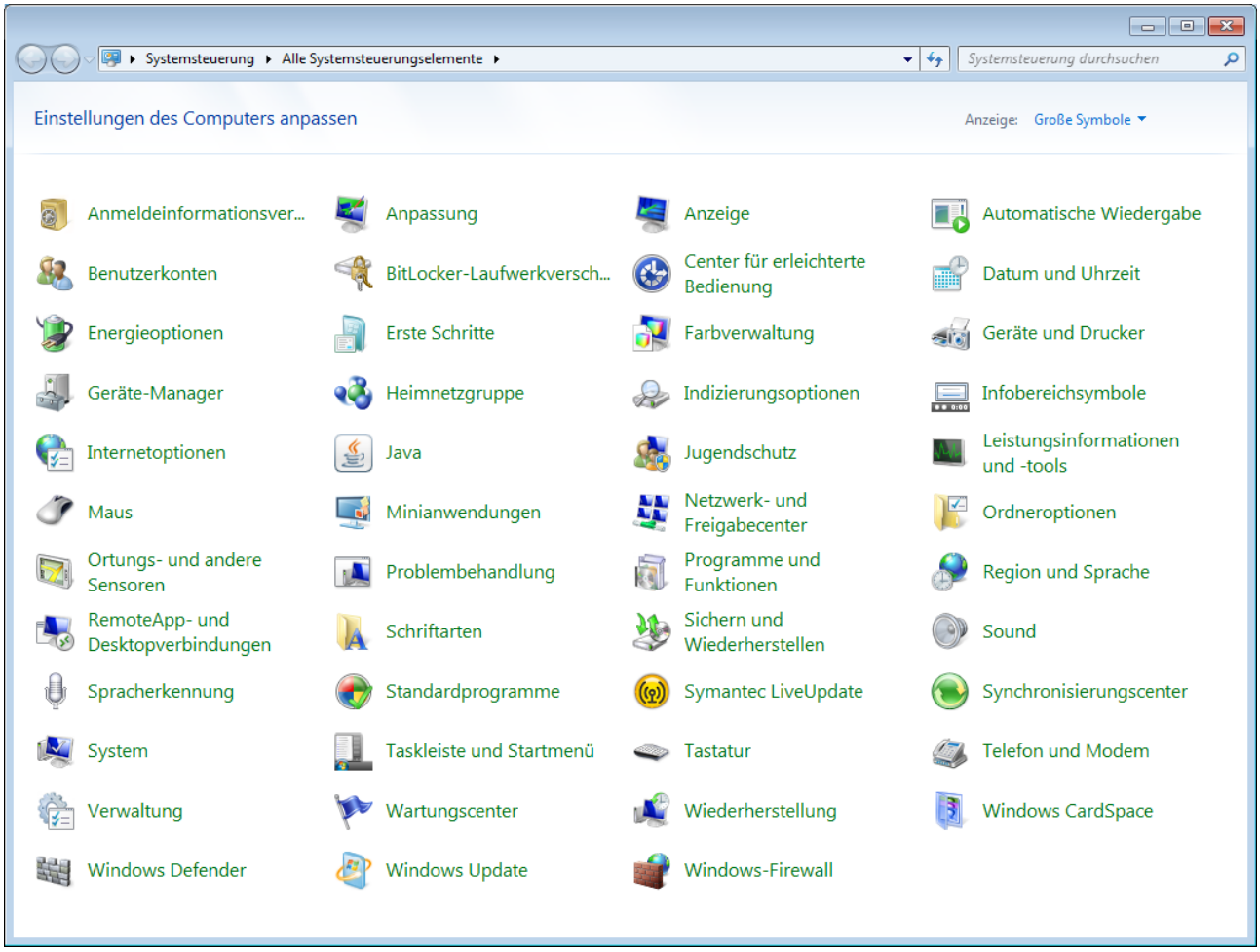


Abbildung 2.3: Die Systemsteuerung

2.2.3 Microsoft Management Console (MMC)

Die Microsoft Management Console (MMC) ist eine grafische Anwendung zur Vereinfachung und Anpassung von administrativen Vorgängen auf Windows-Betriebssystem. Unter Windows 7 wird die Version 3.0 verwendet[23]. Durch Module (sog. Snap-Ins) können administrative Vorgänge individuell zu einem angepassten Werkzeug zusammengebaut werden. Diese Module sind in verschiedene Bereiche unterteilt[24]:

- Benutzerverwaltung: Verwaltung von Benutzern und lokalen Gruppe
- Ressourcenverwaltung: Bearbeitung von System-, Hardware und Softwareeinstellungen
- Dienstverwaltung: Verwaltung und Einstellung von Diensten und deren Eingenschaften
- Ereignisverwaltung: Anzeige aufgetretener Ereignisse
- Geräteüberwachung: Statusüberwachung der lokalen Geräte und Aktualisierung
- Speicherverwaltung: Anzeige und Verwaltung von logischen Plattenlaufwerken
- Anwendungsinstallation: Zentrale Verwaltung und Verteilung von Anwendungen

23 http://msdn.microsoft.com/en-us/library/ms692750(v=vs.85).aspx
24 http://msdn.microsoft.com/en-us/library/ms692748(v=VS.85).aspx

Um die MMC zu starten, ist über dem Windows Startsymbol der Befehl `mmc` einzugeben und ein Rechts-Klick durchzuführen.

Im sich darauf hin öffnenden Fenster (Abbildung 2.4) können mittels Datei → Snap-In hinzufügen/entfernen die benötigten Verwaltungsmodule geladen werden. Durch die Eingabe des entsprechenden Namens des Snap-Ins mit der Dateiendung `.msc` in der Eingabeaufforderung kann das gewünschte Modul auch direkt gestartet werden. Nachfolgender Befehl öffnet das Fenster zur Einstellung der lokalen Sicherheitsrichtlinien: `c:> secpol.msc`

Um die vorhandenen Module zu ermitteln, kann in der Eingabeaufforderung im Wurzelverzeichnis folgender rekursive Befehl abgesetzt werden: `c:> dir *.msc /s`

Weitere Informationen zur Verwendung der MMC mit Windows 7 können unter http://technet.microsoft.com/en-us/library/cc709659.aspx nachgelesen werden.

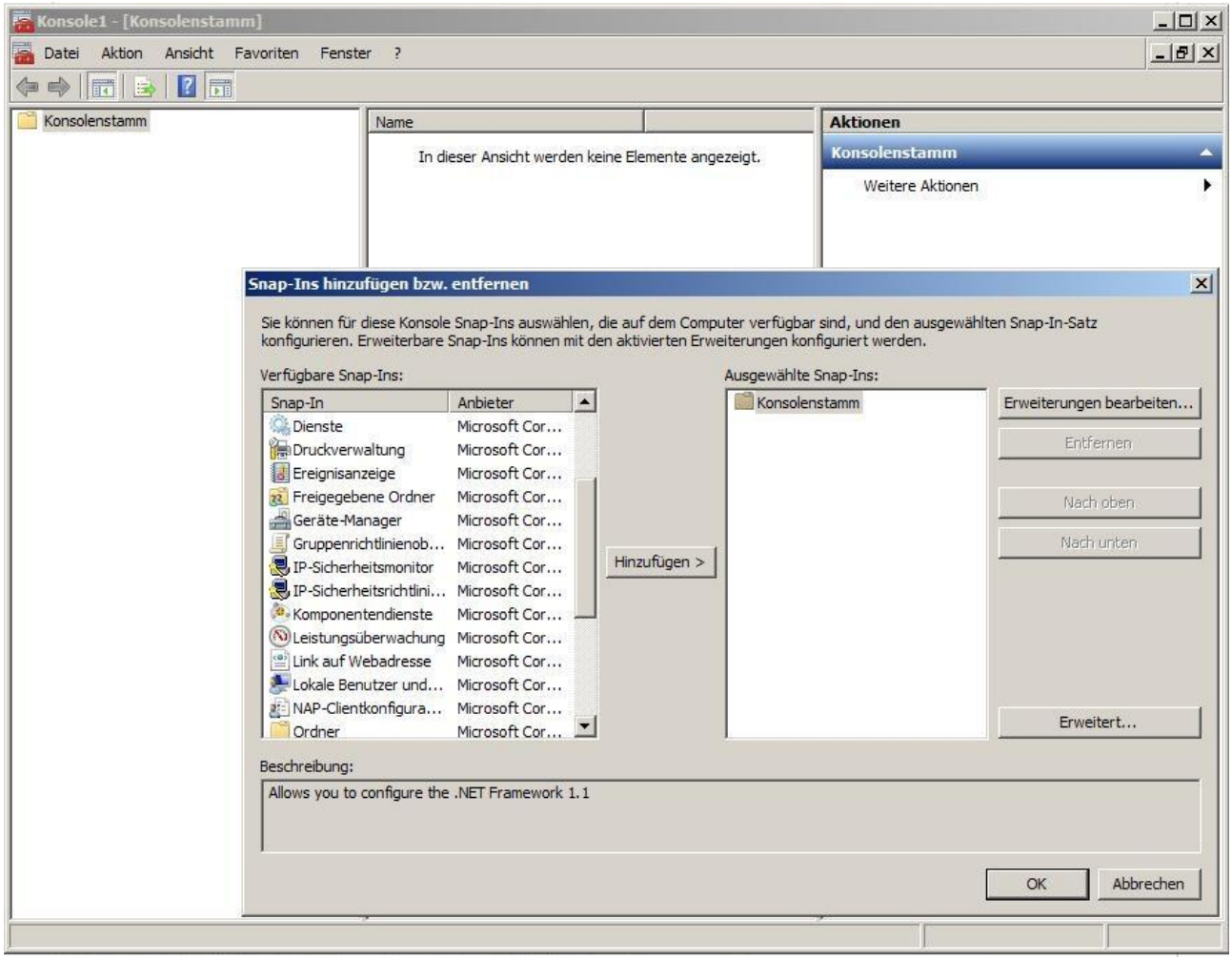


Abbildung 2.4: Microsoft Management Console mit verfügbaren Snap-Ins

2.2.4 Windows Management Instrumentation (WMI)

Die Windows Management Instrumentation (WMI)[25] ist eine administrative Umgebung zur Verwaltung von Daten und Betriebssystemen. Über die WMI können direkt Befehle, Programme oder

aber auch Skripte ausgeführt werden (z. B. C++[26], .NET[27], PowerShell[28], VisualBasic[29] u.a.). Das WMI nutzt das sog. Common Information Model (CIM), einen Industriestandard zur Verwaltung von Anwendungen, Netzwerkkomponenten, aktuellen Betriebssystemen und anderen Komponenten.

Damit über die WMI direkte Befehle ausgeführt werden können, wird das dafür entwickelte Kommandozeilenprogramm WMIC (Windows Management Instrumentation Commandline)[30] benötigt. Durch die Eingabe des Befehls `wmic` in der Eingabeaufforderung wird der interaktive[31] Kommandointerpreter gestartet (Abbildung 2.5). Weitere Informationen zum Arbeiten mit der WMIC sind unter http://technet.microsoft.com/en-us/library/bb742610.aspx#ECAA und unter http://msdn.microsoft.com/en-us/library/aa394531.aspx nachzulesen.

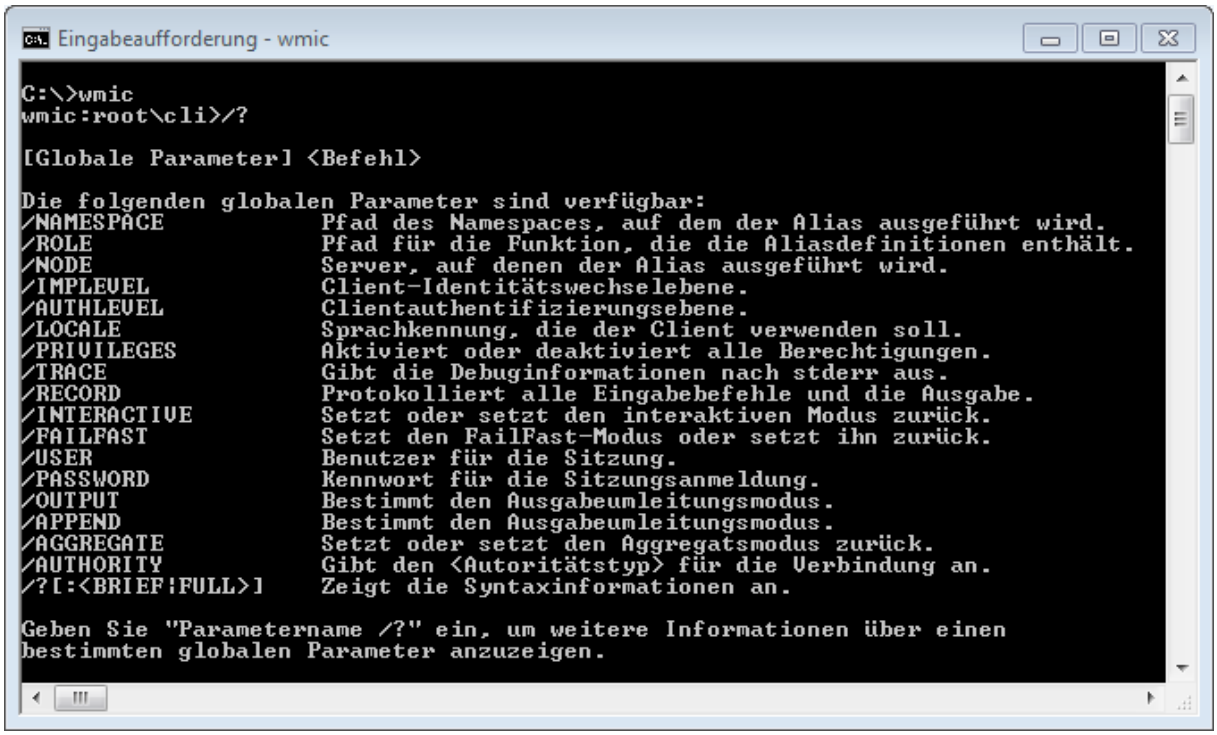


Abbildung 2.5: Windows Management Instrumentation Commandline

2.2.5 Registry

Die Registrierungsdatenbank (Registry)[32] ist die zentrale Konfigurationsdatenbank von Windows Betriebssystemen. In ihr werden Einstellungen des Betriebssystems, der Benutzer und der installierten Anwendungen gespeichert.

Die Registry lässt sich mit einem Editor bearbeiten, der über Start → Ausführen → `regedit.exe` gestartet wird. Zum Bearbeiten der Registry sind Administratorrechte erforderlich. Viele der in Abschnitt 4 vorgenommenen Einstellungen werden direkt in der Registrierungsdatenbank vorgenommen. Vor der Durchführung von Änderungen wird dringend empfohlen einen Export der

26 http://msdn.microsoft.com/en-us/library/aa389762(v=vs.85).aspx
27 http://msdn.microsoft.com/en-us/library/ms257340.aspx
28 http://technet.microsoft.com/de-de/library/aa973757(VS.85).aspx
29 http://msdn.microsoft.com/en-us/library/aa393258(v=vs.85).aspx
30 http://technet.microsoft.com/en-us/library/bb742610.aspx
31 http://blogs.technet.com/b/askperf/archive/2008/04/18/wmic-leveraging-the-power-of-wmi.aspx
32 http://support.microsoft.com/kb/256986

Registrierungsdatenbank durchzuführen, um im Bedarfsfall den ursprünglichen Zustand wieder herstellen zu können. Dies geht entweder über die GUI oder über die Kommandozeile[33].

Die Registry ist hierarchisch aufgebaut und in fünf Hauptzweige unterteilt. Der wichtigste Schlüsselzweig ist `HKEY_LOCAL_MACHINE`. In diesem Zweig werden alle Einstellungen der Windowskonfiguration des APC festgelegt. Im Zweig `HKEY_CURRENT_USER` befinden sich alle Einstellungen des gerade angemeldeten Benutzers.

Bei Windows 7 64-bit besteht die Registry aus einen 32-bit Teil und einen 64-bit Teil. Zugriffe von 32-bit Applikation auf `HKEY_LOCAL_MACHINE\Software` werden in den Zweig `HKEY_LOCAL_MACHINE\Software\Wow6432Node` umgeleitet. Dies geschieht mit Hilfe des sog. Registry Redirectors[34] und ist für die entsprechenden Applikationen transparent.

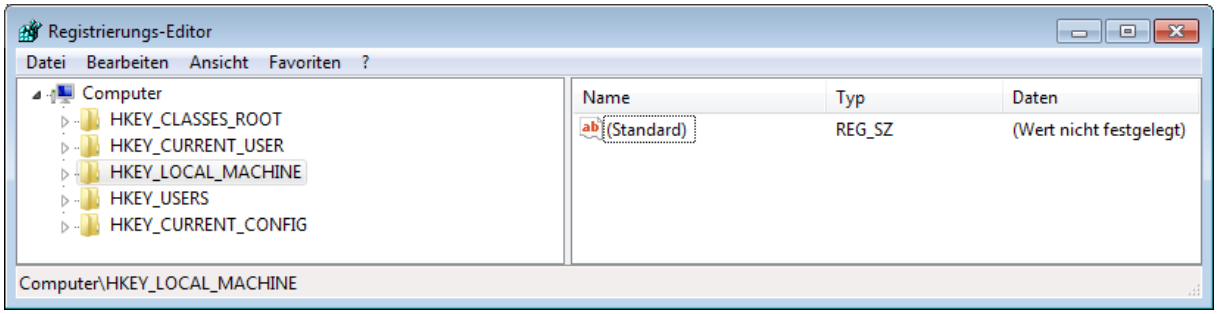


Abbildung 2.6: Der Registrierungs-Editor

2.2.6 Die Gruppenrichtlinie (GPO)

Über Gruppenrichtlinien oder Group Policy Objects[35] (GPOs) lassen sich ähnlich der Registrierungsdatenbank diverse Programmeinstellungen setzen oder Sicherheitseinstellungen anwenden. Dabei wird grundsätzlich zwischen Domänenrichtlinien und lokale Richtlinien unterschieden. Mittels Domänenrichtlinien lassen sich mehrere APC, die einer Domäne angehören, gleich konfigurieren. Lokale Gruppenrichtlinien werden nur auf dem zu konfigurierenden APC angewendet und nicht an andere APC verteilt.

Die Gruppenrichtlinien werden in einer GUI konfiguriert, die sich lokal über Start → Ausführen → `gpedit.msc` aufrufen lässt. Auch hier sind Administratorrechte erforderlich. Die Einstellungen sind zu einem großen Teil mit Hilfetexten versehen. Mit den Gruppenrichtlinien lässt sich ein APC übersichtlicher administrieren als dies mit dem Registrierungseditor möglich ist. Zusätzlich zum Editor für die Gruppenrichtlinien gibt es noch weitere Werkzeuge für die Kommandozeile[36]. Damit lassen sich beispielsweise die Gruppenrichtlinien direkt oder zu einem bestimmten Zeitpunkt aktualisieren.

33 http://technet.microsoft.com/en-us/library/cc736340%28WS.10%29.aspx
34 http://technet.microsoft.com/en-us/library/aa384232(VS.85).aspx
35 http://technet.microsoft.com/en-us/library/hh147307%28WS.10%29.aspx
36 http://technet.microsoft.com/de-de/library/cc728172%28WS.10%29.aspx

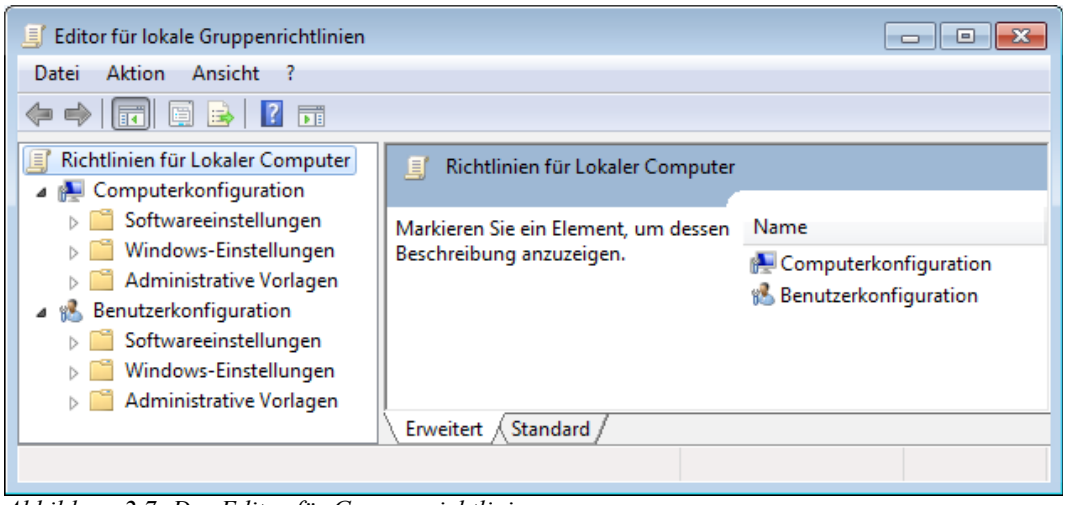


Abbildung 2.7: Der Editor für Gruppenrichtlinien

2.3 Sicherheitsfunktionen

Windows 7 stellt zahlreiche Sicherheitsfunktionen bereit, die den Schutz des Betriebssystems gegenüber Angriffen verbessern und den Schutz vor Datenabfluss zu erhöhen. Auf die wichtigsten Sicherheitsfunktionen wird nachfolgend eingegangen.

2.3.1.1 Bitlocker

Die mit Microsoft Windows Vista eingeführte Festplattenverschlüsselung namens *Bitlocker Drive Encryption* (kurz BDE oder BitLocker) ist auch in Windows 7 verfügbar, jedoch nur in den Versionen Ultimate und Enterprise. Mittels BitLocker werden NTFS Volumes mit dem Advanced Encryption Standard (AES) verschlüsselt[37]. Voraussetzung für die Verschlüsselung mittels BitLocker ist dabei entweder ein TPM Chip (Trusted Platform Module) oder ein USB-Stick, auf dem der Schlüssel gespeichert wird[38]. Die Ver- und Entschlüsselung der Datenpartitionen erfolgt nach der Konfiguration für den Anwender unbemerkt im Hintergrund.

Seit Windows 7 gibt es zusätzlich zum BitLocker die Software *Bitlocker To Go*, mit der Wechseldatenträger wie USB-Sticks oder externe Festplatten verschlüsselt werden können. Für BitLocker To Go ist weder ein TPM noch ein USB-Token zwingend erforderlich. Um Daten auf einem anderen Windows-Betriebssystem (z. B. Windows XP) öffnen zu können, wird lediglich das BitLocker To Go-Lesetool benötigt[39].

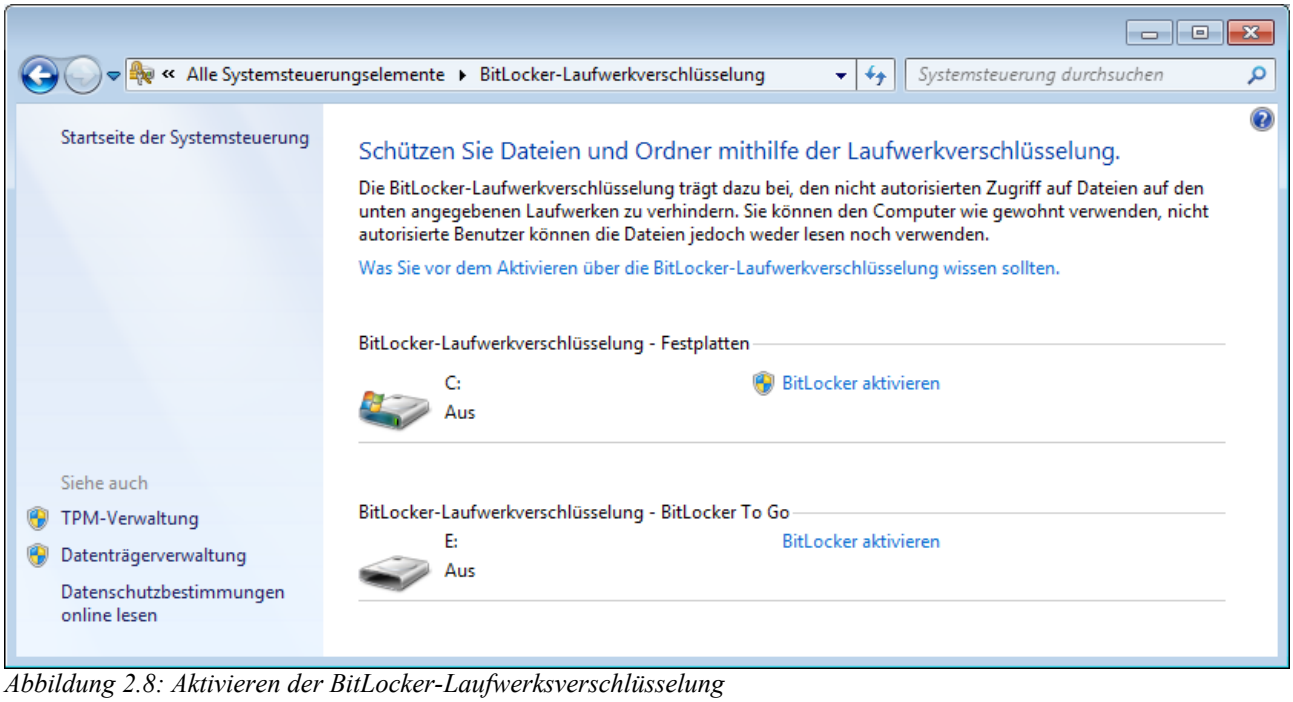


Abbildung 2.8: Aktivieren der BitLocker-Laufwerksverschlüsselung

37 http://technet.microsoft.com/de-de/library/dd548341(WS.10).aspx
38 BitLocker Drive Encryption im mobilen und stationären Unternehmenseinsatz vom Fraunhofer Institut / BSI
39 http://www.microsoft.com/downloads/de-de/details.aspx?FamilyID=64851943-78c9-4cd4-8e8d-f551f06f6b3d&displaylang=de

2.3.2 Encrypting File System (EFS)

Eine weitere Möglichkeit zur Datenverschlüsselung ist das *Encrypting File System* (EFS)[40], das schon länger in den Microsoft Betriebssystemen XP und Server 2000 enthalten ist[41]. Es setzt auf einem NTFS Dateisystem auf und ermöglicht es, einzelne Dateien und Ordner auf einer Festplatte zu verschlüsseln. Windows 7 verwendet dabei AES zur Verschlüsselung.

Jede Datei wird mit dem sog. File Encrypting Key verschlüsselt. Dieser Schlüssel wird asymmetrisch mit dem öffentlichen Schlüssel des Benutzers verschlüsselt[42]. Zum Entschlüsseln wird der private Schlüssel des Benutzers verwendet. Beide Schlüssel sind in Zertifikaten auf der Festplatte des APC abgelegt. Andere Benutzer können mittels EFS verschlüsselte Dateien zwar öffnen, jedoch nicht entschlüsseln. Da EFS nur einzelne Dateien oder Pfade verschlüsselt, stellt dies keine Alternative zur Festplattenverschlüsselung (z. B. BitLocker) dar.

2.3.2.1 AppLocker

Mit Windows 7 hat Microsoft neue Möglichkeiten zur Ausführungskontrolle von Programmen und Anwendungen implementiert. Auf dieses Feature ist nur in den Versionen Ultimate und Enterprise vorhanden. Mit der Anwendung *AppLocker*[43] können nunmehr Zugriffe für Benutzer oder Gruppen über Gruppenrichtlinienobjekte konfiguriert werden. Die konfigurierbaren Regeln basieren auf Signatur-[44] und Attributeigenschaften der Anwendung. Um AppLocker auf dem APC nutzen zu können, ist der Dienst Anwendungsidentität zu starten. Zum automatischen Starten ist der Starttyp von Manuell auf Automatisch zu ändern. Über Gruppenrichtlinienobjekte kann AppLocker zentral konfiguriert werden. Abbildung 2.10 zeigt diese Konfigurationsmöglichkeit.

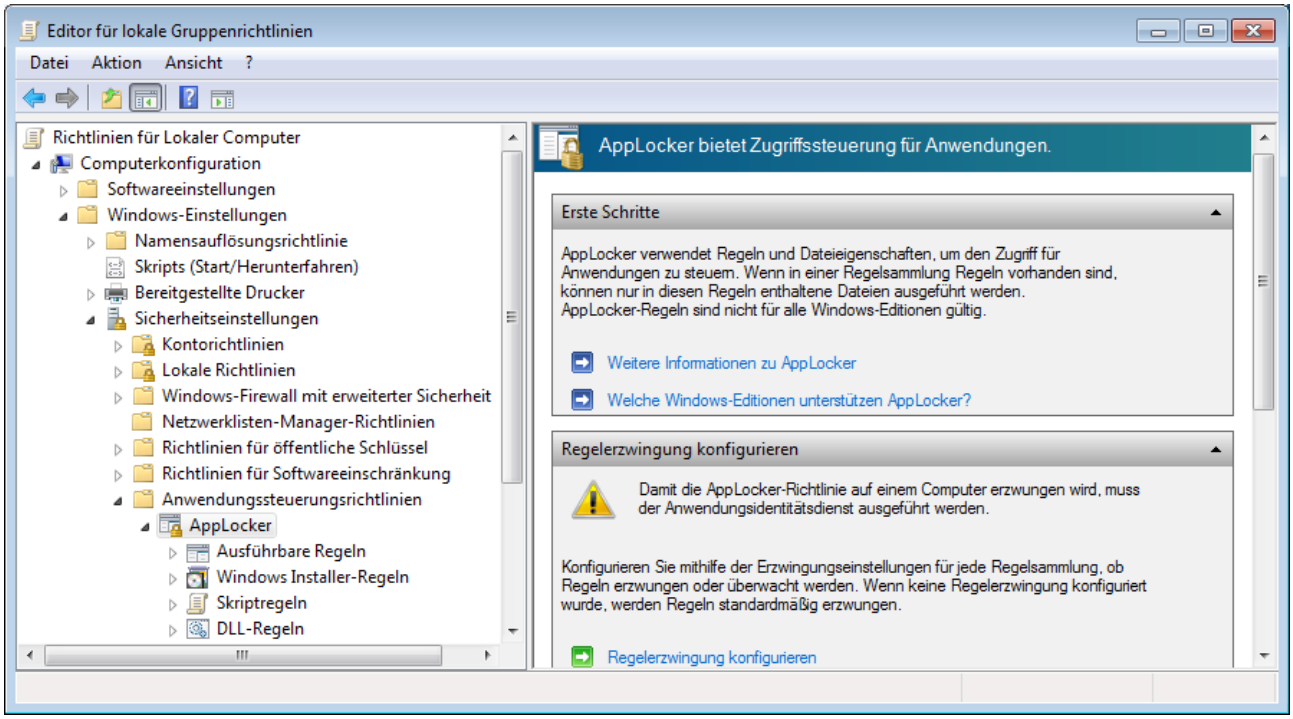


Abbildung 2.9: Konfiguration von AppLocker

Das Regelwerk für AppLocker ist in vier Gruppen unterteilt:

40 http://www.microsoft.com/germany/technet/datenbank/articles/900941.mspx
41 http://technet.microsoft.com/en-us/library/bb457020.aspx
42 BitLocker Drive Encryption im mobilen und stationären Unternehmenseinsatz vom Fraunhofer Institut / BSI
43 http://technet.microsoft.com/en-us/library/ee424367(WS.10).aspx
44 http://technet.microsoft.com/en-us/library/dd723683(WS.10).aspx

- Ausführbare Regeln gelten für die Dateiformate `.exe` und `.com`. Hier wird festgelegt, welche Programme ausführbar sind bzw. nicht ausgeführt werden dürfen[45].
- Windows Installer Regeln legen fest, wer Windows Installer Setups ausführen darf und gelten für die Dateiformate `.msi` und `.msp`[46].
- Scriptregeln gelten für die Dateiformate `.ps1`, `.bat`, `.cmd`, `.vbs` und `.js` und erlauben die Ausführung von Scripten[47].
- DLL-Regeln gelten für die Dateiformate `.dll` und `ocx` und erlauben die Steuerung auf DLLs[48]. Die Darstellung der DLL-Konfiguration ist standardmäßig nicht sichtbar. Erst durch die folgende Aktion im Gruppenrichtlinieneditor wird dieser Konfigurationspunkt dargestellt: Rechtsklick auf AppLocker → Eigenschaften → Erweitert → Hacken bei „DLL Regelsammlung aktivieren“ setzen.

Für eine Regel gilt, dass diese die Ausführbarkeit zulässt oder diese verweigert[49]. Diese Eigenschaft kann Benutzern oder Gruppen zugewiesen werden.

2.3.2.2 Benutzerkontensteuerung

In früheren Windows-Versionen arbeiteten viele Benutzer standardmäßig mit hoch privilegierten Rechten. Dadurch bedingt wurden automatische Installationen von Programmen nicht erkannt. Um dies zu vermeiden gibt es in Windows 7 die *User Access Control* (UAC)[50] [51]. Durch diese Funktion in Ihrer Standardeinstellung werden Anwender immer über Vorgänge informiert, welche eine administrative Berechtigung benötigen (z. B. Installation eines Programmes).

45 http://technet.microsoft.com/de-de/library/ee460956(WS.10).aspx
46 http://technet.microsoft.com/de-de/library/ee460957(WS.10).aspx
47 http://technet.microsoft.com/de-de/library/ee460958(WS.10).aspx
48 http://technet.microsoft.com/de-de/library/ee460947(WS.10).aspx
49 AppLocker kontrolliert keinen interpretierten Programmcode (z. B. Office Macro, Perl), keine Anwendungen außerhalb des Win32 Subsystems (z. B. POSIX) und keine 16-bit DOS Binaries. Es werden nur die hier angegebenen Dateiformate unterstützt. Wird aus einem nicht unterstützen Dateiformat (z. B. .bin) eine Aktion aufgerufen (z. B .exe), welche durch AppLocker kontrolliert werden kann, dann greift die definierte Regel.
50 http://technet.microsoft.com/en-us/library/cc731416%28WS.10%29.aspx
51 http://technet.microsoft.com/de-de/library/ee679793(WS.10).aspx

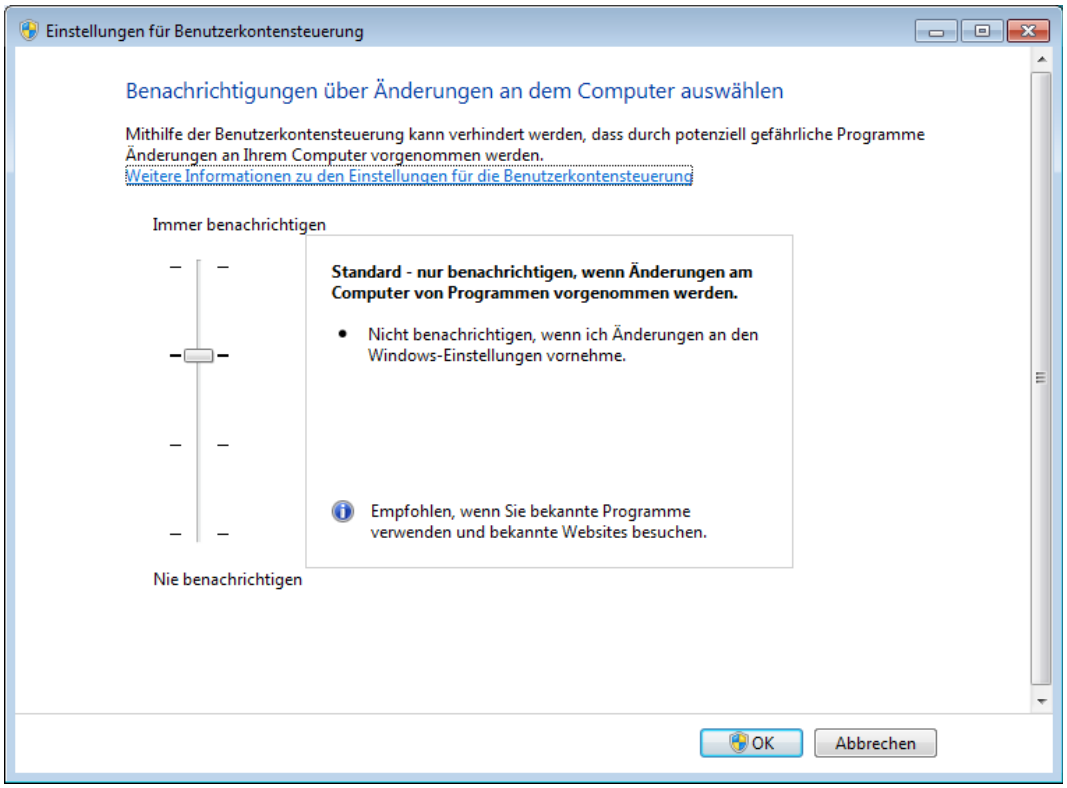


Abbildung 2.10: Einstellungen der Benutzerkontensteuerung

In der UAC sind folgende Einstellungen möglich:

Immer benachrichtigen:

> Möchte ein Programm Änderungen am Computer oder Ihr Benutzerkonto Einstellungen am System vornehmen, so wird der Benutzer benachrichtigt und muss dieser Aktion zustimmen oder diese ablehnen. Diese Einstellung ist die sicherste und bedarf einer häufigeren Interaktion.

Nur benachrichtigen, wenn Änderungen an meinem Computer von Programmen vorgenommen werden (Standardeinstellung):

> Eine Benachrichtigung erfolgt nur, wenn ein Programm versucht Änderungen am Computer vorzunehmen für welche administrative Berechtigungen nötig sind. Bei Änderungen an Systemeinstellungen werden keine Benachrichtigungen ausgegeben. Ändert eine Schadprogramm nur die Systemkomponenten, so wird der Anwender über diesen Vorgang nicht informiert.

Nur benachrichtigen, wenn Änderungen an meinem Computer von Programmen vorgenommen werden (Desktop nicht abblenden):

> Eine Benachrichtigung erfolgt nur, wenn ein Programm versucht Änderungen am Computer vorzunehmen für welche administrative Berechtigungen nötig sind. Bei Änderungen an Systemeinstellungen werden keine Benachrichtigungen ausgegeben. Diese Benachrichtigungen werden nicht im sicheren Desktop angezeigt. Somit können andere Programme ausgeführt werden, welche die Benachrichtigung möglicherweise beeinträchtigen können.

Nie benachrichtigen:

Es erfolgt keine Benachrichtigung über die von Programmen vorgenommenen Aktionen oder Einstellungen am Betriebssystem. Benötigen Programme Administrationsberechtigungen unter einem nicht administrativen Benutzerkonto, so wird das Programm nicht ausgeführt. Diese Einstellung ist als unsicher einzustufen. Daher sollte diese nicht verwendet werden.

Anmerkungen: Es gilt weiterhin der Grundsatz, dass normale Benutzer keine Administrationsrechte auf dem System haben dürfen.

2.3.3 Datenausführungsverhinderung

Bedingt durch Programmierfehler kann es unter gewissen Umständen beim Verarbeiten von Daten dazu kommen, dass die zu verarbeitenden Daten länger als die im Programm dafür vorgesehenen Datenstrukturen sind. Wird keine exakte Längenprüfung der zu verarbeitenden Daten durchgeführt, können unter Umständen andere, nicht für diese Daten vorgesehene Speicherbereiche eines Programms überschrieben werden. So kann z. B. der Stack, ein Teil des Arbeitsspeichers, der als temporärer Speicher für aufgerufene Funktionen innerhalb eines Programms dient, überschrieben werden.

Solche Überläufe werden häufig unter der Bezeichnung *Puffer-Überläufe* (engl. Buffer-overflows) zusammengefasst und können überall dort auftreten, wo Daten eingelesen und bearbeitet werden. *Speicherschutzmechanismen* (Executable Space Protection, ESP) unterbinden die Ausführung von Programmen aus nicht dafür zugelassenen Bereichen des Arbeitsspeichers. Dazu werden über Mechanismen des Prozessors Speicherbereiche als „nicht ausführbar“ markiert. Voraussetzung für das Funktionieren dieses Mechanismus sind Dienste und Anwendungen, die nicht darauf angewiesen sind, ihre eigenen Datenbereiche als Code auszuführen.

Im Windows-Umfeld trifft das nicht auf alle Programme zu. Daher wird der Speicherschutz bei Windows (*Data Execution Prevention*, DEP) standardmäßig bei XP, Vista und Windows 7 nur für Windows-Systemdateien eingesetzt[52].

Um zu überprüfen, welche Systemprogramme DEP verwenden, kann eine Abfrage mit dem Zusatzprogramm Process Explorer[53] durchgeführt werden (siehe Abbildung 2.11).

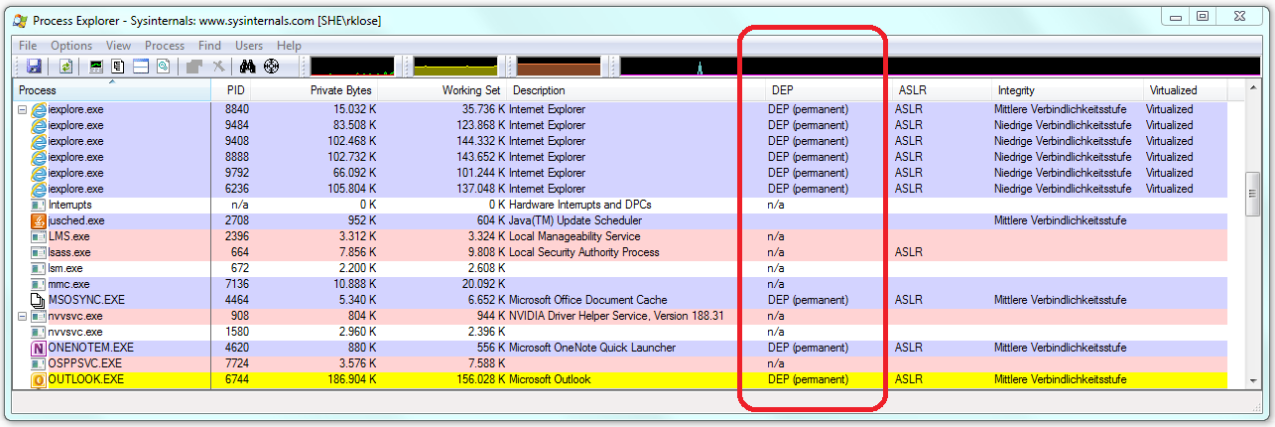


Abbildung 2.11: Der Prozess-Explorer zeigt an, welche Prozesse DEP verwenden.

2.3.4 Speicherrandomisierung

Kennt der Angreifer den Aufbau des laufenden Programms im Arbeitsspeicher, kann er den Programmfluss durch einen Puffer-Überlauf auch an eine Stelle im Code dirigieren, die ihm dienliche Aktionen ausführt. Die Speicherrandomisierung (Address Space Layout Randomization, ASLR) sorgt dafür, dass der Angreifer möglichst wenig Wissen über die Struktur des Programms

52 http://support.microsoft.com/kb/875352
53 http://technet.microsoft.com/de-de/sysinternals/bb896653

im Arbeitsspeicher erhält, indem die beim Start eines Programms geladenen, dynamischen Bibliotheken zufällig im Adressraum verteilt werden.

Dies erschwert einem Angreifer, Einsprungadressen in Bibliotheks- und Anwendungsfunktionen zu ermitteln. Sowohl die dynamischen Bibliotheken als auch die darauf zugreifenden Anwendungen müssen ASLR-fähig sein. Betriebssystemanwendungen von Windows 7 verwenden standardmäßig eine Speicherrandomisierung. Zusätzlich installierte Anwendungen unterstützen diese Funktion nur, wenn dies durch den Hersteller implementiert wurde. Um zu überprüfen, welche Anwendungen ASLR verwenden, kann eine Abfrage mit dem Zusatzprogramm Process Explorer[54] betrachtet werden (siehe Abbildung 2.12).

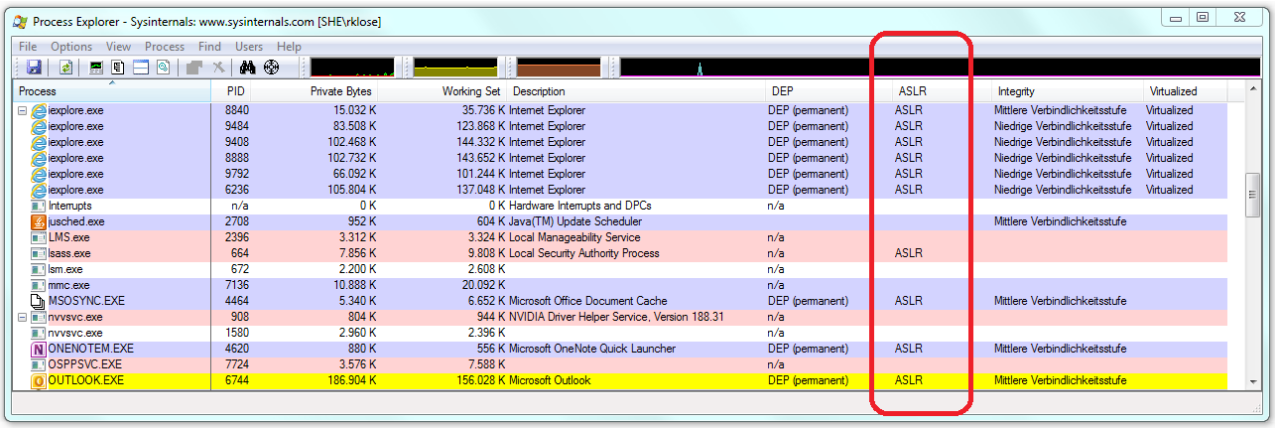


Abbildung 2.12: Der Prozess-Explorer zeigt an, welche Prozesse ASLR verwenden.

2.3.5 Automatische Updates

Die regelmäßige Aktualisierung von Betriebssystem und Anwendungen ist eine wesentliche Schutzmaßnahme gegenüber Angriffen, weil durch Aktualisierungen häufig Sicherheitslücken geschlossen werden. Dazu lädt der Windows-Update Manager über das Netz neue Versionen des Betriebssystem-Kerns, der Bibliotheken, der Dienste oder der mit dem Betriebssystem mitgelieferten Anwendungen und installiert diese.

Das Laden kann grundsätzlich von zwei verschiedenen Quellen erfolgen:

- Aktualisierungen werden über das Internet direkt von einem Web-Server des Herstellers geladen.
- Die APCs im lokalen Netz beziehen ihre Aktualisierungen von einem lokalen Update-Server, der Aktualisierungen seinerseits vom Hersteller über das Internet lädt.

Die standardmäßige Einstellung, wie mit Updates verfahren werden soll, kann während der Installation festgelegt werden und nachträglich über die Systemeinstellungen angepasst werden.

Es können die vier folgenden Vorgehensweisen unter dem Bereich „Wichtige Updates“ gewählt werden:

- Updates automatisch installieren (empfohlen):

  Die verfügbaren Updates werden ermittelt, heruntergeladen und automatisch installiert. Hierzu kann ein zeitliches Intervall festgelegt werden. Ist der APC zu diesem Zeitpunkt nicht angeschaltet, wird die Aktion beim nächsten Systemstart durchgeführt und die Installation beim nächsten Herunterfahren des Betriebssystems gestartet.
- Updates herunterladen, aber Installation manuell durchführen:

  Die verfügbaren Updates werden ermittelt und heruntergeladen, jedoch muss die Installation durch den Benutzer gestartet werden. Hierzu kann ein zeitliches Intervall fest-

54 http://technet.microsoft.com/de-de/sysinternals/bb896653

gelegt werden. Ist der APC zu diesem Zeitpunkt nicht angeschaltet, wird die Aktion *Ermitteln und herunterladen* beim nächsten Systemstart durchgeführt. Der Anwender wird über die Verfügbarkeit von aktuellen und nicht installierten Updates benachrichtigt und Updates werden herunter geladen. Die Installation der Updates ist manuell durchzuführen.

- Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren manuell festlegen:

  Die verfügbaren Updates werden ermittelt, jedoch wird die Software-Komponente nur mittels einer manuelle Interaktion durch den Benutzer heruntergeladen und installiert. Hierzu kann ein Zeitliches Intervall festgelegt werden. Ist der APC zu diesem Zeitpunkt nicht angeschaltet, wird die Aktion *Ermitteln* beim nächsten Systemstart durchgeführt. Der Anwender wird über die Verfügbarkeit von aktuellen Updates auf dem definierten Update-Server benachrichtigt.
- Nie nach Updates suchen (nicht empfohlen):

  Diese Einstellung deaktiviert die automatische Aktualisierungsfunktion.

2.3.5.1 Windows-Firewall

Seit Windows XP ist die Windows-Firewall ein integraler Bestandteil des Betriebssystems. Windows 7 bietet gegenüber früheren Versionen neue Konfigurationsmöglichkeiten. Diese sogenannte erweiterte Sicherheitsfunktion[55] erlaubt die Definition verschiedener Profile. Diese Profile steuern das Netzwerkverhalten abhängig von der Netzwerkumgebung (Domäne, lokales Netz oder öffentliches Netz) und sind auf einzelne Netzwerkkarten anwendbar (Abbildung 2.15).

So können beispielsweise für unterschiedliche Netzwerkkarten unterschiedliche Firewall-Regeln definiert und zugewiesen werden. Die Regeln sind frei definierbar und lassen sich auf Programme und/oder Ports anwenden. Ist der APC dann mittels einer kabelgebundenen Schnittstelle einem Netzwerk beigetreten (z. B. Firmennetzwerk), können andere Regeln greifen als dies möglicherweise an einem öffentlichen und kabellosen Zugangspunkt (Hotspot) möglich sein sollte[56].

55 http://technet.microsoft.com/en-us/library/cc748991(WS.10).aspx
56 http://technet.microsoft.com/de-de/library/cc755158(WS.10).aspx

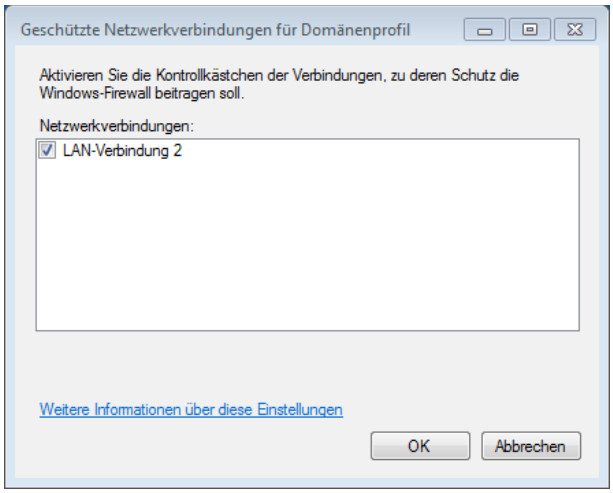


Abbildung 2.13: Zuordnung eines Profils zu einer Netzwerkverbindung

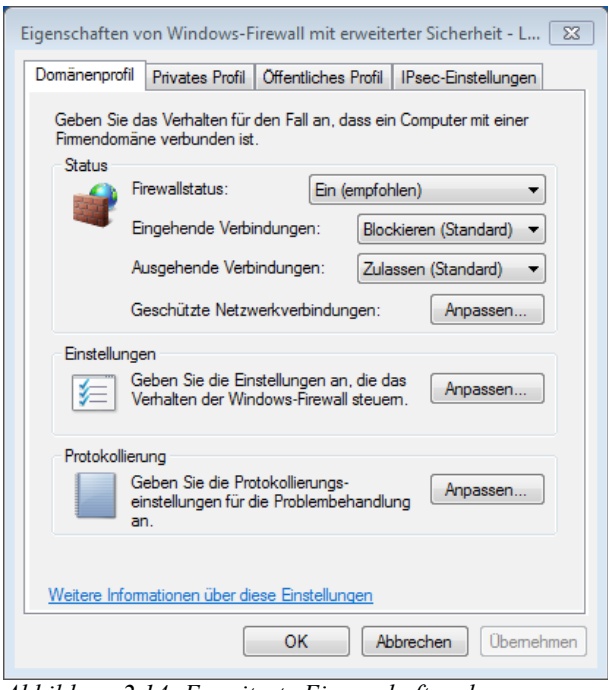


Abbildung 2.14: Erweiterte Eigenschaften der Windows-Firewall

2.4 System-Dienste

Dienste sind Programme, die im Hintergrund von Windows 7 laufen und lokal für andere Komponenten des Betriebssystems und Anwendungsprogrammen oder sogar über das Netz Funktionen zur Verfügung stellen. Bei Unix- oder Linux-Systemen spricht man von Daemons und bei Windows von System-Diensten[57]. Während einige Dienste bereits mit dem Betriebssystem ausgeliefert werden, können andere Dienste auch als Teil einer Anwendungen nachträglich installiert werden.

Windows 7 bietet mehrere Möglichkeiten, die vorhandenen Dienste zu ermitteln:

1. WMIC: Die WMIC (Windows Management Instrumentation Commandline) ist ein Kommandozeilenprogramm, welches die Systemkomponenten verwalten kann[58]. Folgendes Kommando speichert eine Liste der lokalen Dienste mit allen verfügbaren Informationen in einem HTML-Dokument auf dem Laufwerk `C:\` gespeichert.

   ```
   WMIC /OUTPUT:"C:\Service_all.htm" Service GET /FORMAT:htable
   ```

2. MMC: Die MMC (Microsoft Management Console) ist ein Verwaltungsprogramm zur Administration von Systemkomponenten über eine grafische Oberfläche[59]. Wird Folgendes Kommando[60] in der `CMD.exe` ausgeführt, werden alle lokalen Dienste mit allen verfügbaren Informationen aufgeführt und sind veränderbar: `services.msc`

3. Systemsteuerung: Alle Dienste können ebenfalls über Systemsteuerung / Verwaltung[61] / Computerverwaltung / Dienste aufgerufen werden:

57 Mit dem Begriff „Dienst“ werden auch Leistungen bezeichnet, die von Servern über ein Netz angeboten werden. Typische Beispiele für solche Dienste sind E-Mail, WWW und DHCP. Im Folgenden ist mit „Dienst“ ein Hintergrundprozess gemeint.
58 http://www.microsoft.com/austria/technet/articles/wmic.mspx
59 http://technet.microsoft.com/en-us/library/bb742442.aspx
60 Das folgende Kommando im Wurzelverzeichnis `C:>` listet alle vorhandenen Snap-Ins auf: `dir *.msc /s`
61 Hierzu von der Anzeige „Kategorie“ auf „Symbole“ gewechselt werden, damit der Punkt „Verwaltung“ direkt erreichbar wird.

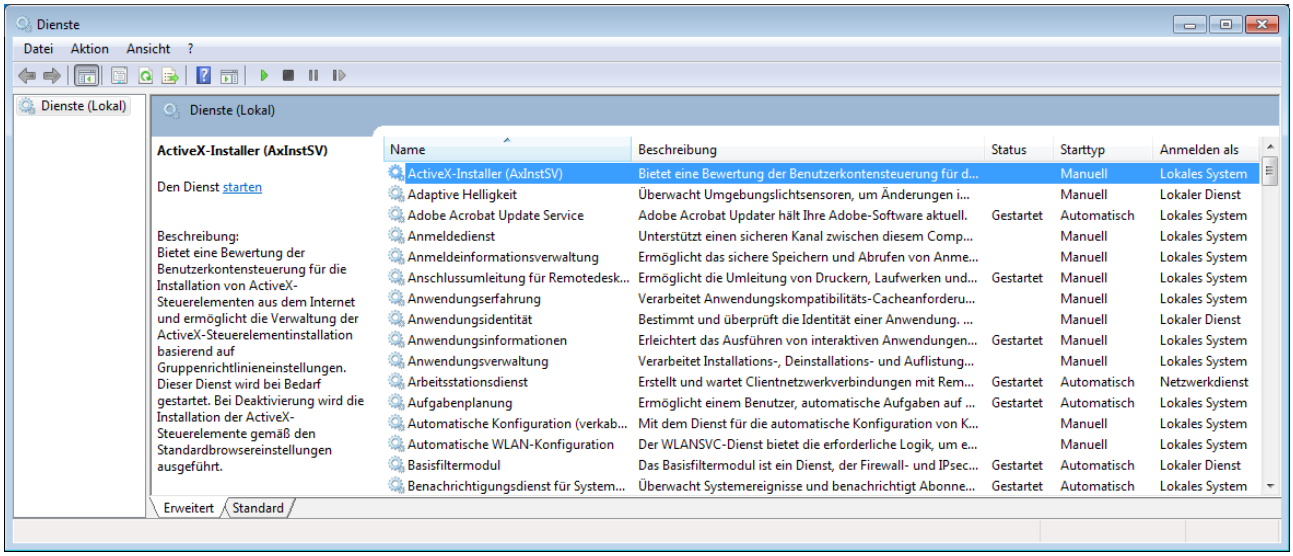


Abbildung 2.15: Verwaltung der Dienste über die Systemsteuerung

Tabelle 13 listet die einzelnen Dienste eines neu installierten Windows 7 auf und gibt eine Übersicht der Abhängigkeiten[62]. Die Werte in den Spalten Starttyp und Gestartet entsprechen jeweils den Standardeinstellungen. Diese werden in Abschnitt 4.3 angepasst.

62 http://www.winfaq.de/faq_html/Content/tip2500/onlinefaq.php?h=tip2668.htm

Dienst	*Starttyp*[63]	*Gestartet*[64]	*Ist Abhängig von*	*Wird genutzt von*
Arbeitsstationsdienst	A	J	Browsersupporttreiber Netzwerkspeicher-Schnittstellendienst SMB 1.x - Miniredirector SMB 2.0 - Miniredirector	Anmeldedienst Computerbrowser Konfiguration für Remotedesktops
Anwendungserfahrung	M	J	--	--
ActiveX-Installer (AxInstSV)	M	N	Remoteprozeduraufruf (RPC)	
Adaptive Helligkeit	M	N	--	--
Anmeldedienst	M	N	Arbeitsstationsdienst	--
Anmeldeinformationsverwaltung	M	N	Remoteprozeduraufruf (RPC)	Internetbrowser Windows-Biometrie-dienst
Anschlussumleitung für Remotedesktopdienst im Benutzer-modus.	M	N	--	Terminaldienste
Anwendungsidentität	M	N	--	Anwendungs-ID-Treiber Kyptografiedienste Remoteprozeduraufruf (RPC)
Anwendungsinformationen	M	J	Benutzerprofildienst Remoteprozeduraufruf (RPC)	--
Anwendungsverwaltung	M	N	--	--
Aufgabenplanung	A	J	Remoteprozeduraufruf (RPC) Windows-Ereignis-protokoll	Per Aufgabenplanung gesteuerte Dienste
Automatische Konfiguration (ver-kabelt)	M	N	Extensible Authertication-Protokoll, NDIS Usermode I/O Protocol, Remoteprozeduraufruf (RPC)	--
Automatische WLAN-Konfiguration	M	N	Extensible Authertication-Protokoll, NativeWiFi-Filter, NDIS Usermode I/O Protocol Remoteprozeduraufruf (RPC)	--
Basisfiltermodul	A	J	Remoteprozeduraufruf (RPC)	Gemeinsame Nutzung der Internetverbindung,

63 Starttyp: A für Automatisch, M für Manuell
64 Gestartet: J für Status „gestartet“, N für Status „gestoppt“

Dienst	*Starttyp*	*Gestartet*	*Ist Abhängig von*	*Wird genutzt von*
				IKE- und AuthIP IPsec-Schlüsselerstellungsmodule, Ipsec-Richtlinien-Agent, Routing und RAS; Windows-Firewall
Benachrichtigungsdienst für Systemereignisse	A	J	COM+ Ereignissystem	COM+ Systemanwendung
Benutzerprofildienst	A	J	Remoteprozedurenaufruf (RPC)	Anwendungsinformationen
BitLocker-Laufwerkverschlüsselungsdienst.	M	N	TPM (Hardwarechip in der Version 1.2)	--
Blockebenen-Sicherungsmodul	M	N	--	--
Bluetooth-Unterstützungsdienst	M	N	Remoteprozedurenaufruf (RPC)	--
BranchCache	M	N	Http	--
CNG-Schlüsselisolation	M	N	Remoteprozedurenaufruf (RPC)	Extensible Authentification-Protocol
COM+-Ereignissystem	A	J	Remoteprozedurenaufruf (RPC)	Benachrichtigungsdienst für Systemereignisse COM+-Systemanwendung DFS-Replikation, Intelligenter Hintergrundübertragungsdienst, SL-Benutzerschnittstellen-Benachrichtigungsdienst
COM+-Systemanwendung	M	N	Benachrichtigungsdienst für Systemereignisse COM+-Ereignissystem Remoteprozedurausruf (RPC)	--
Computerbrowser	M	N	Arbeitsstationsdienst Server	--
DCOM-Server-Prozessstart.	A	J	–	Remoteprozeduraufruf (RPC)
Defragmentierung.	M	N	Remoteprozeduraufruf (RPC)	--
Designs.	A	J	–	--
DHCP-Client	A	J	Ancillary Function Driver for Winsock, NetIO-Legacy-TDI-Supporttreiber Netzwerkspeicher-Schnittstellendienst	WinHTTp-Web Proxy Auto-Discovery-Dienst
Diagnosediensthost	M	J	–	--

Dienst	*Starttyp*	*Gestartet*	*Ist Abhängig von*	*Wird genutzt von*
Diagnoserichtliniendienst	A	J	–	--
Diagnosesystemhost	M	N	–	--
Distributed Transaction Coordinator	M	N	Remoteprozeduraufruf (RPC) Sicherheitskonto-Manager	--
DNS-Client	A	J	NetIO-Legacy-TDI-Supporttreiber	Dienste welche zur Kommunikation DNS benötigen
Druckwarteschlange	A	J	HTTP Remoteprozeduraufruf (RPC)	FAX
Enumeratordienst für tragbare Geräte	M	J	Rempteprozedurenaufruf (RPC)	Media-Player Bildimport-Assistent
Erkennung interaktiver Dienste	M	N	–	Interaktive Dialogfelder von interaktiven Diensten
Extensible Authentication-Protokoll	M	N	CNG-Schlüsselisolation Remoteprozeduraufruf (RPC)	Automatische Konfiguration (ver-kabelt) Automatische WLAN-Konfiguration
Fax	M	N	--	Druckerwarteschlange Plug & Play Remoteprozeduraufruf (RPC) Telefonie
Funktionssuchanbieter-Host	M	N	HTTP Remoteprozeduraufruf (RPC)	PnP-X-IP-Busauflistung Windows-Media-Center
Funktionssuche-Ressourcenveröffent-lichung	M	N	HTTP Remoteprozedureaufruf (RPC)	Heimnetzgruppen-An-bieter
Gatewaydienst auf Anwendungsebene	M	N	--	Gemeinsame Nutzung der Internetverbindung
Gemeinsame Nutzung der Internet-verbindung	aus-geschaltet	N	Basisfiltermodul Netzwerkverbindungen RAS-Verbindungsver-waltung Windows-Verwaltungs-instrumentation	--
Geschützter Speicher	M	N	Remoteprozeduraufruf (RPC)	--
Gruppenrichtlinienclient	A	J	Mup Remoteprozedureaufruf (RPC)	--
Heimnetzgruppen-Anbieter	M	N	Funktionssuchanbieter-Host Funktions-suche-Ressourcenver-	--

Dienst	*Starttyp*	*Gestartet*	*Ist Abhängig von*	*Wird genutzt von*
			öffentlichung Netzwerklistendienst	
Heimnetzgruppen-Listener	M	N	Server	--
IKE- und AuthIP Ipsec-Schlüsselerstellungsmodule	M	N	Basisfiltermodul	IPsec-Dienste
Integritätsschlüssel- und Zertifikatverwaltung	M	N	Remoteprozeduraufruf (RPC)	NAP
Intelligenter Hintergrundübertragungsdienst	M	J	COM+Ereignissystem Remoteprozeduraufruf (RPC)	Wiederaufnahme eines abgebrochenen Downloads
IP-Hilfsdienst	A	J	NetIO-Legacy-TDI-Supporttreiber Netzwerkspeicher-Schnittstellendienst Remoteprozeduraufruf (RPC) TCP/IP-Protokolltreiber Windows-Verwaltungsinstrumentation	IPv6-Kommunikation
IPsec-Richtlinien-Agent	M	N	Basisfiltermodul TCP/IP-Protokolltreiber	--
Konfiguration für Remotedesktops	M	N	Arbeitsstationsdienst Remoteprozeduraufruf (RPC)	--
Kryptografiedienste	A	J	Remoteprozeduraufruf (RPC)	Funktionsbeeinträchtigung der Verwaltungsdienste
KtmRm für Distributed Transaction Coordinator	M	N	Remoteprozeduraufruf (RPC) Sicherheitskonto-Manager	--
Leistungsindikator-DLL-Host	M	N	Remoteprozeduraufruf (RPC)	--
Leistungsprotokolle und -warnungen	M	N	Remoteprozeduraufruf (RPC)	--
Media Center Extender-Dienst	ausgeschaltet	N	Funktionssuchanbieter-Host PnP-X-IP-Busauflistung SSDP-Suche Terminaldienste	--
Microsoft .NET Framework NGEN v2.0.50727_X64.	M	N	--	--
Microsoft iSCSI-Initiator-Dienst	M	N	--	--
Microsoft-Softwareschattenkopie-Anbieter	M	N	Remoteprozeduraufruf (RPC)	Systemwiederherstellung
Multimediaklassenplaner	A	N	--	Windows-Audio
NAP-Agent (Network Access Protection)	M	N	Remoteprozeduraufruf	NAP-Funktion der Domäne
Net.Tcp-Portfreigabedienst	aus-	N	--	--

Dienst	*Starttyp*	*Gestartet*	*Ist Abhängig von*	*Wird genutzt von*
	geschaltet			
Netzwerklistendienst	M	J	NLA (Network Location Awareness) Remoteprozeduraufruf (RPC)	SL-Benutzerschnitt-stellen-Be-nachrichtigungsdienst
Netzwerkspeicher-Schnittstellendienst	A	J	NSI-Proxy service	Arbeitsstationsdienst; DHCP-Client IP-Hilfsdienst Netzwerkverbindungen NLA (Network Location Awareness)
Netzwerkverbindungen	M	J	Netzwerkspeicher-Schnittstellendienst Remoteprozeduraufruf (RPC)	Gemeinsame Nutzung der Internetverbindung
NLA (Network Location Awareness)	A	J	Netzwerkspeicher-Schnittstellendienst Remoteprozeduraufruf (RPC) TCP/IP-Protokolltreiber	Netzwerklistendienst
Offlinedateien	A	J	Remoteprozeduraufruf (RPC)	--
Parental Controls	M	N	Remoteprozeduraufruf (RPC)	--
Peer Name Resolution-Protokoll	M	N	Peernetzwerkidentitäts-Manager	Peernetzwerk-Gruppenzuordnung PNRP-Computernamenveröffen tlichungs-Dienst Windows-Teamarbeit Dateiverteilungs-programme
Peernetzwerk-Gruppenzuordnung	M	N	Peer Name Resolution-Protokoll Peernetzwerkidentitäts-Manager	Windows-Teamarbeit
Peernetzwerkidentitäts-Manager	M	N	--	Peer Name Resolution-Protokoll Peernetzwerk-Gruppenzuordnung Windows-Teamarbeit Dateiverteilungs-programme
Plug & Play	A	J	--	Fax Smartcard Tablet PC-Eingabedienst Telefonie Virtueller Datenträger Windows Driver Foundation – Benutzermodus-Treiberframework

Dienst	*Starttyp*	*Gestartet*	*Ist Abhängig von*	*Wird genutzt von*
				Windows Modules Installer Windows-Audio-Endpunkteerstellung
PnP-X-IP-Busenumerator	M	N	Funktionssuchanbieter-Host Remoteprozeduraufruf (RPC)	Windows Media Center
PNRP-Computernamenveröffentlichungs-Dienst	M	N	Peer Name Resolution-Protokoll	–
Programmkompatibilitäts-Assistent-Dienst	A	J	Remoteprozeduraufruf (RPC)	Programm Compatibility Assistant
RAS-Verbindungsverwaltung	M	N	Telefonie	Gemeinsame Nutzung der Internetverbindung Routing und RAS Verwaltung für automatische RAS-Verbindung
Remotedesktopdienste	M	N	Remoteprozedur -Aufruf (RPC) Terminal-Gerätetreiber	Anschlussumleitung für Terminaldienst im Benutzermodus Media Center Extender-Dienst schnelle Benutzerumschaltung Remoteunterstützung Remotedesktop
Remoteprozeduraufruf (RPC)	A	J	OM-Server-Prozessstart	Nahezu allen anderen Dienste
Remoteregistrierung	M	N	Remoteproceduraufruf (RPC)	--
Richtlinie zum Entfernen der Scmartcard	M	N	Remoteproceduraufruf (RPC)	--
Routing und RAS	ausgeschaltet	N	Basisfiltermodul NetBIOSGroup; RAS-Verbindungsverwaltung Remoteprozeduraufruf (RPC)	--
RPC-Endpunktzuordnung	A	J	--	Remoteprozeduraufruf (RPC)
RPC-Locator	M	N	--	--
Sekundäre Anmeldung	M	N	--	--
Server für Threadsortierung	M	N	--	--
Server	A	J	Sicherheitskonto-Manager srv	Computerbrowser
Shellhardwareerkennung	A	J	Remoteprozeduraufruf (RPC)	Windows-Bilderfassung

Dienst	*Starttyp*	*Gestartet*	*Ist Abhängig von*	*Wird genutzt von*
Sicherheitscenter	A	J	Remoteprozeduraufruf (RPC) Windows-Verwaltungs-instrumentation	--
Sicherheitskonto-Manager.	A	J	Remoteprozeduraufruf (RPC)	Distributed Transaction Coordinator für Distributed Transaction Coordinator Server
Sitzungs-Manager für Desktopfenster-Manager	A	J	--	AERO
Smartcard	M	N	Plug und Play	Fingerabdruck-Leser
SNMP-Trap	M	N	--	Netzwerküberwachungssoftware
Software Protection	A	J	Remoteprozeduraufruf (RPC)	Lizenzierter Windowssoftware
Speicherdienst	M	N	--	--
SPP-Benachrichtigungsdienst	M	J	COM+-Ereignissen	--
SSDP-Suche	M	J	HTTP	UpnP-Gerätehost Mediageräte im Netzwerk
SSTP-Dienst	M	N	--	RAS-Verbindungsverwaltung
Stromversorgung	A	J	--	Akku Energiesparmodus von Festplatte, Monitor, usw. Windows-Audio-Endpunkt-erstellung
Superfetch	M	N	File Information FS MiniFilter Remoteprozeduraufruf (RPC)	--
Tablet PC-Eingabedienst	M	N	Plug u. Play Remoteprozeduraufruf (RPC)	Berührungsempfindliche oberfläche
TCP/IP-NetBIOS-Hilfsdienst	A	J	Ancilliary Function Driver for Winsock; NETBT	Anzeige von Schattenkopien Kommunikation mit Windows 95 APCs
Telefonie	M	N	Plug u. Play Remoteprozeduraufruf (RPC)	Fax RAS-Verbindugsverwaltung Verwaltung für automatische RAS-Verbindung Softwaretelefonie
TPM-Basisdienste	M	N	--	BitLocker
Überwachung verteilter Verknüpfungen (Client)	A	J	Remoteprozeduraufruf (RPC)	--

Dienst	*Starttyp*	*Gestartet*	*Ist Abhängig von*	*Wird genutzt von*
Unterstützung in der Systemsteuerung unter Lösungen für Probleme	M	N	--	--
UPnP-Gerätehost	M	N	HTTP SSDP-Suche	Windows Media Player-Netzwerkfreigabedienst
Verbessertes Windows-Audio/Video-Streaming	M	N	Link-Layer Topology Discovery Mapper I/O Driver QoS-Paketplaner QWAVE-Treiber Remoteprozeduraufruf (RPC)	Streaming-Software
Verbindungsschicht-Topologie-erkennungs-Zuordnungsprogramm	M	N	Link-Layer Topology Discovery Mapper I/O Driver Remoteprozeduraufruf (RPC)	--
Verschlüsselndes Dateisystem (EFS)	M	N	Remoteprozeduraufruf (RPC)	Anwendungen, die auf verschlüsselte Dateien zugreifen möchten
Verwaltung für automatische RAS-Verbindung	M	N	RAS-Verbindugsverwaltung Telefonie	Dial-UP oder DSL-Internetverbindungen
Virtueller Datenträger	M	N	Plug u. Play Remoteprozeduraufruf (RPC)	--
Volumeschattenkopie	M	N	Remoteprozeduraufruf (RPC)	Dateiwiederherstellung
WebClient	M	N	--	WebDAV Funktionen
Windows CardSpace	M	N	--	--
Windows Defender	A	J	Remoteprozeduraufruf (RPC)	--
Windows Driver Foundation - Benutzermodus-Treiberframework	A	J	Plug und Play	Verifikation von Windows-Treibern
Windows Installer	M	N	Remoteprozeduraufruf (RPC)	Softwareverwaltung
Windows Media Center-Empfänger-dienst	M	N	Remoteprozeduraufruf (RPC)	Windows Media Center
Windows Media Center-Planerdienst	M	N	Remoteprozeduraufruf (RPC)	Windows Media Center
Windows Media Player-Netzwerk-freigabedienst	M	N	HTTP UPnP-Gerätehost	Windows Media Center Windows Media Player
Windows Modules Installer	M	N	Plug und Play	Möglicherweise Fehler beim Windows-Update
Windows Presentation Foundation-Schriftartcache 3.0.0.0	M	N	--	WPF-Anwendungen
Windows Search	A	J	Remoteprozeduraufruf (RPC)	--

Dienst	*Starttyp*	*Gestartet*	*Ist Abhängig von*	*Wird genutzt von*
Windows Update	A	J	Remoteprozeduraufruf (RPC)	--
Windows-Audio	A	J	Multimediaklassenplaner Remoteprozeduraufruf (RPC) Windows-Audio-End-punkterstellung Multimediaklassenplaner	Windows-Media-Center Windows-Media-Player Audio-Software
Windows-Audio-Endpunkterstellung	A	J	Plug und Play Stromversorgung	Windows-Audio
Windows-Bilderfassung (WIA)	M	N	Remoteprozeduraufruf (RPC) Shellhardwareerkennung	--
Windows-Biometriedienst.	M	N	Anmeldeinformationsverwaltung Remoteprozeduraufruf (RPC) Windows Driver Foundation - Benutzermodus-Treiberframework	Biometrischer Authentifizierung
Windows-Dienst für Schriftartencache	M	N	--	--
Windows-Ereignisprotokoll	A	J	--	Aufgabenplanung
Windows-Ereignissammlung	M	N	--	--
Windows-Farbsystem	M	N	Remoteprozeduraufruf (RPC)	Bildverarbeitungssoftware
Windows-Fehlerberichterstattungs-dienst.	M	N	Remoteprozeduraufruf (RPC)	--
Windows-Firewall.	A	J	Basisfiltermodul Windows-Firewall-autorisierungstreiber	--
Windows-Remoteverwaltung (WS-Verwaltung)	M	N	HTTP Remoteprozeduraufruf (RPC)	WMI
Windows-Sicherung	M	N	Remoteprozeduraufruf (RPC)	Backup und System-wiederherstellung
Windows-Sofortverbindung - Konfigurationsregistrierungsstelle	M	N	Remoteprozeduraufruf (RPC)	Netzwerkkonfiguration
Windows-Verwaltungsinstrumentation	A	J	Remoteprozeduraufruf (RPC)	Gemeinsame Nutzung der Internetverbindung IP-Hilfsdienst Sicherheitscenter
Windows-Zeitgeber	M	N	--	Zertifikatsdienste
WinHTTP-Web Proxy Auto-Discovery-Dienst	M	J	DHCP-Client	Internet-Zugang über diverse Protokolle (z. B. HTTP(s), FTP,...)
WMI-Leistungsadapter	M	N	--	WMI-Remoteabfragen
WWAN - automatische Konfiguration	M	N	NDIS Usermode I/O Protokol	--

Dienst	*Starttyp*	*Gestartet*	*Ist Abhängig von*	*Wird genutzt von*
			NLA (Network Location Awareness) Plug & Play Remoteprozeduraufruf (RPC)	
Zertifikatverteilung	M	N	Remoteprozeduraufruf (RPC)	Smartcard-Leser und abhängigen Diensten
Zugriff auf Eingabegeräte	M	N	--	--

Tabelle 13: Windows Dienste

2.5 Zusätzliche Anwendungen

Neben den von Microsoft Windows 7 mitgelieferten Softwarekomponenten wie dem Media Player und dem Internet Explorer sollen bei Bedarf weitere Anwendungsprogramme auf dem APC installiert werden können. Die Installation zusätzlicher Anwendungen muss auch nach der Minimierung weiterhin möglich sein.

Für den im Rahmen dieses Dokuments betrachteten Büro-APC sollen standardmäßig folgende Anwendungen installiert werden:

- Windows Media Player
- Microsoft Internet Explorer
- Alternativer Internet-Browser
- Software zur Textverarbeitung
- PDF Reader zur Anzeige von PDF-Dateien
- Packer zum Komprimieren und Dekomprimieren von Dateien

Zur Installation dieser weiteren Anwendungen wird der Windows-Installations-Dienst (msiserver) benötigt.

Wird eine zusätzliche Anwendung installiert oder betrieben, kann diese Anwendung unter Umständen Änderungen in den Einstellungen des Betriebssystems vornehmen. Dies können beispielsweise das Starten von Diensten oder das Freischalten von Kommunikationsverbindungen in der Windows-Firewall sein. Daher sollten alle nachträglich installierten Anwendungen evaluiert, überwacht und auf ihre Sicherheit hin untersucht werden.

3 Installation des Betriebssystems

Im Abschnitt 2 wurde die Architektur von Microsoft Windows 7 beschrieben und auf die technischen Unterschiede der verfügbaren unterschiedlichen Versionen näher eingegangen.

Dieser Abschnitt beschreibt die Installation des Microsoft Betriebssystems Windows 7 Professional 64-Bit.

3.1 Vorbereitung der Installation

Bevor die Installation eines APC vorgenommen wird, sind nachfolgend beschriebene, vorbereitende Tätigkeiten durchzuführen.

- Überprüfung der Vertrauenswürdigkeit einer aus dem Internet heruntergeladen ISO-Abbilddatei anhand des SHA-1 oder MD5 Hash-Wertes. Mit dem Microsoft Befehlszeilenprogramm FCIV (File Checksum Integrity Verifier) sollte der kryptografische Hash -Wert MD5 oder SHA-1 berechnet sowie in einer XML-Dateidatenbank für spätere Verwendung gespeichert werden.[65] Somit lässt sich die Integrität des ISO-Abbilds verifizieren, aus dem dann ein Installationsmedium erstellt werden kann.
- Bei der Verwendung eines gekauften Originaldatenträgers sind die aufgebrachten Kopierschutzkennzeichnung auf ihr Vorhandensein sowie die Unversehrtheit des Siegels zu überprüfen[66].
- Bei der Installation über einen Bereitstellungsdienst von Windows ist darauf zu achten, dass das richtige Startabbild, das zu installierende Installationsabbild sowie ein vertrauenswürdiges PXE-Netzwerk zur Verfügung stehen. Durch entsprechende Absicherungen wie z. B. der Verwendung eines dedizierten PXE-Netzwerks in dem nur bekannte Clients PXE und DHCP Anfragen stellen dürfen, kann der Zugriff auf PXE basierende Installationen reglementiert bzw. bestimmten Clients zugeordnet werden.
- Es wird empfohlen, nicht mehrere Betriebssysteme auf einem APC parallel zu installieren um einen Austausch von Daten ohne entsprechende Rechte zu vermeiden. Weiterhin wird empfohlen, diese Installationsanweisung ausschließlich auf einem APC anzuwenden, der den Vorgaben aus [ISi-Client] entspricht.
- Das Sichern von eventuell auf dem lokalen Datenspeicher gespeicherten Daten soll vor möglichem Datenverlust schützen, wenn z. B. eine Neuinstallation eines APC durchgeführt werden soll.
- Der APC muss die Voraussetzungen für die Hardware-Kompatibilitätsliste[67] von Microsoft erfüllen.
- Die Bootreihenfolge für die entsprechende Installationsvariante ist festzulegen.
- Für die Installation von Windows 7 ist die Partitionierung sowie die Formatierung zu beachten. Eine Windows 7 Version kann nur auf einen Datenträger installiert werden, der mit dem Dateisystem NTFS formatiert wurde. Die Festplatte wird außerdem noch mit einer Disk-Signatur im MBR (Master Boot Record) versehen. Windows 7 benötigt diese Disk-Signatur, um die Datenträger zu identifizieren und um Laufwerksbuchstaben für

65 http://support.microsoft.com/kb/841290
66 http://www.microsoft.com/HowToTell/
67 http://www.microsoft.com/windows/compatibility/windows-7/de-de/default.aspx

Partitionen zu vergeben[68]. Die Disk-Signatur wird von Windows beim Initialisieren eines Datenträgers automatisch vergeben. Partitionierte und formatierte Festplatten, die keine Disk-Signatur enthalten, werden als unbekannte Datenträger klassifiziert, deren Formatierung mit NTFS obligatorisch ist. NTFS formatierte Datenträger mit einer Disk-Signatur werden vom Setup erkannt und können bei einem Upgrade erhalten werden. Bei einer Neuinstallation wird auch diese Partition mit NTFS formatiert.

Auf fabrikneuen Datenträgern gibt es häufig eine separate Partition, die typischerweise Wiederherstellungswerkzeug der Festplatte oder spezielle Software und Treiber für das System enthält. Diese Partitionen werden in der Regel nicht benötigt und sollten gelöscht und formatiert werden.

- Microsoft empfiehlt als Minimalvoraussetzung bei einem Windows 7 Professional 64-Bit eine Festplattengröße von 20 GB. Weiterhin werden 100 MB für das System reserviert und stehen somit dem Anwender nicht zur Verfügung (siehe auch Tabelle 4 auf Seite 11).
- Die Namen des ersten lokalen Benutzers und des Computers müssen festgelegt werden. Ebenso ist die Bestimmung des aktuellen Standortes des APCs erforderlich.
- Es muss ein gültiger Windows-Produkt Schlüssel bereit gestellt werden.

68 http://technet.microsoft.com/en-us/library/cc977219.aspx

3.2 Verschiedene Installationsvarianten

In diesem Abschnitt werden kurz die notwendigen Schritte für die Durchführung einer Erstinstallation eines APC mit dem Betriebssystem Microsoft Windows 7 beschrieben. Wenn Möglichkeiten bestehen, bei einer initialen Installation Betriebssystemkomponenten wirksam zu deaktivieren bzw. von vornherein nicht mitzuinstallieren, wird an entsprechender Stelle hierauf hingewiesen. Darüber gehend hinaus wird in Abschnitt 4 beschrieben, wie die Minimalisierung des Systems durchzuführen ist.

Grundsätzlich gibt es verschiedene Möglichkeiten der Betriebssysteminstallation:

- In Abschnitt 3.2.1 wird die Installationsvorgehensweise mit einem Medium wie z. B. DVD beschrieben.
- Abschnitt 3.2.2 geht auf eine Installation des Betriebssystem mit einem vorgefertigten Image ein.
- In dem Abschnitt 3.2.3 wird die automatisierte Installation von Windows Clients mittels Netzwerkinstallation beschrieben.

Der Installationsprozess wird in diesem Dokument in die drei Phasen unterteilt: Pre-Installations-, Systeminstallations- und Post-Installations-Phase. In der Pre-Installationsphase besteht die Möglichkeit, die Erstkonfiguration des Systems gesteuert durch eine Antwortdatei oder durch den Administrator vorzunehmen. In der Systeminstallationsphase wird dann die eigentliche Installation sowie das automatische Kopieren der Windowsdateien des Betriebssystems durchgeführt. Die Post-Installationsphase wird dazu genutzt, entsprechende nachträgliche Konfigurationen an dem System vorzunehmen. Nachträgliche Konfigurationen können abhängig von der Installationsvariante entweder durch einen Administrator vorgenommen oder mittels einer Antwortdatei unbeaufsichtigt durchgeführt werden.

3.2.1 Installation via Installationsmedium

Für die Installation des APC ist der Computer von einem bootfähigem Medium zu starten. Gegebenenfalls ist die Bootreihenfolge zu ändern, wobei das CD/DVD Laufwerk als Erstes auszuwählen ist. Hierbei sind die Einstellungen im BIOS individuell zu berücksichtigen.

In dieser Phase sind grundsätzliche Einstellungen vorzunehmen.

3.2.1.1 Pre-Installationsphase

Folgende Systemschritte sind durchzuführen:

1. Booten von einem Windows 7 Medium (z. B. DVD oder CD)
2. Nach dem Bootvorgang wird das Windows-Setup gestartet.
3. Abfrage der Windows-Installation, die durch die unteren drei Punkte zu beantworten und mit Weiter zu bestätigen sind:
    1. Auswahl der Installationssprache: Hier wird die Sprache für die Installation ausgewählt.
    2. Eingabe der Uhrzeit und des Währungsformats: Auswahl der Uhrzeit des APC und des Währungsformats (hierdurch wird beispielsweise das Währungssymbol festgelegt).
    3. Auswahl ob Tastatur oder Eingabemethode: Hier wird festgelegt, welche Sprache Windows verwenden soll, um Text anzuzeigen.
4. Aufforderung zum Installieren: Durch Bestätigen des Button „Jetzt installieren“ wird das Setup angewiesen, Windows 7 auf den Datenträger des APC zu installieren.

5. Akzeptieren der Lizenzbedingungen: Durch das Aktivieren der Check-Box „Ich akzeptiere die Lizenzbedingungen“ wird den Lizenzbedingungen zugestimmt und der Installationsprozess kann mit dem Button „Weiter“ durchgeführt werden.
6. Auswahl der Installationsart: „Upgrade“ steht für eine Aktualisierung eines bestehenden Betriebssystems und „Benutzerdefiniert (erweitert)“ für eine Neuinstallation:
    1. Upgrade: Aktualisiert ein bestehendes Windows Betriebssystem. Dabei wird keine Neuinstallation vorgenommen, sondern nur die bestehenden Systemdateien durch Windows 7 Systemdateien ersetzt. Die entsprechenden Updatepfade werden in Abschnitt 2.1 beschrieben.
    2. Benutzerdefiniert (erweitert): Mit dieser Installationsart wird ein neues Windows Betriebssystem installiert. Dabei wird eine Formatierung des Datenträgers vorgenommen. Bei einer Formatierung der Festplatte droht eventuell Datenverlust. Daher sollte vor der Formatierung der Festplatte geprüft werden, ob sich Daten auf dem Datenträger befinden (s. h. Abschnitt 3.1). Nach der Auswahl dieser Installationsart ist der Installationsort anzugeben. Die Formatierung mit NTFS wird nach erfolgreicher Partitionierung durchgeführt.
7. Möglicher Installationsort bzw. Partitionierung eines Datenträgers: Dabei wird festgestellt, ob der Datenträger eine für Windows 7 lesbare Partition oder eine noch nicht erstellte Partition enthält. Wird eine nicht unterstützte Version des NTFS-Dateisystems entdeckt, ist diese zu formatieren. Wurde noch keine Partition auf dem Datenträger erstellt, so muss diese erst erstellt werden. Entsprechende Laufwerksoptionen können mit dem Link „Laufwerkoptionen (erweitert)“ angezeigt und genutzt werden. Folgende Optionen stehen zur Verfügung:
    1. Aktualisieren: Damit werden die Datenträger neu eingelesen.
    2. Löschen: Eine ausgewählte Partition wird gelöscht.
    3. Formatieren: Eine ausgewählte Partition wird mit NTFS formatiert.
    4. Neu: Eine neue Partition wird auf dem ausgewählten Datenträger erstellt.
    5. Treiber laden: Zusätzliche Treiber für z. B. RAID- oder SCSI-Controller können geladen werden, um beispielsweise auf weitere oder andere Datenträger zugreifen zu können bzw. Windows zu installieren.
    6. Erweitern: Eine bestehende Partition um weiteren Speicherplatz erweitern.

Datenträger, die noch nicht für eine Windowsinstallation vorbereitet sind, werden als „Nicht zugewiesener Speicherplatz auf Datenträger 0“ angezeigt. Durch Markieren des Datenträgers und bestätigen des „Weiter“ Buttons wird die Kapazitätszugehörigkeit automatisch zugeteilt:

1. Datenträger 0 Partition 1: System-reserviert 100 MB
2. Datenträger 0 Partition 2: Restlicher Speicherbereich

Durch Auswahl des Links „Neu“ erhält man die Möglichkeit die Kapazität für jede gewünschte Partition frei zu bestimmen. Dabei wird immer eine System-reservierte Partition von 100 MB für den Bootmanager von Windows 7 automatisch erstellt. Nach dem Erstellen und Formatieren der Partition wechselt das Setup automatisch in die Systeminstallation.

3.2.1.2 Systeminstallation

Bei der Grundinstallation von Windows 7 sind keine Konfigurationsmöglichkeiten vorhanden. Die Systeminstallation unterteilt sich in die folgenden Punkte, die ohne manuellen Eingriff des Benutzers automatisch durchgeführt werden:

1. Windows-Dateien werden kopiert: Windows-Dateien werden auf den lokalen Datenträger kopiert.
2. Windows-Dateien werden expandiert: Die kopierten Daten werden entpackt.
3. Reboot/Registrierungseinträge werden erstellt.
4. Funktionen werden installiert: Dieser Vorgang installiert Windows-Funktionen.
5. Updates werden installiert: Mögliche Aktualisierungen werden durchgeführt.
6. Installation wird abgeschlossen: Abschluss der Windows-Installation.
7. Reboot des Betriebssystems.

Das Setup wird nach erfolgreichem Reboot weitergeführt. Damit ist die Systeminstallation durchgeführt und das Setup wechselt in die Konfigurationsphase.

3.2.1.3 Post-Installationsphase

Nach der Grundinstallation sind vom Administrator noch Konfigurationen vorzunehmen. Hierfür sind die folgenden Systemschritte durchzuführen:

1. Ersten lokalen Benutzer sowie den Computernamen des APC einrichten: Es müssen diesem APC spezifische Merkmale wie Benutzername und Computername einmalig zugewiesen werden. Mit dem Benutzername wird ein lokaler Account angelegt. Mit dem Computername wird der APC im Netzwerk eindeutig identifiziert:
   a) Eingabe des Benutzernamens
   b) Eingabe des Computernamens
2. Kennwort für den ersten lokalen Benutzer festlegen:
   a) Eingabe eines Kennworts und dessen Wiederholung: Mit der Vergabe des Kennwortes wird dem erstellten Account ein Kennwort zugewiesen. Es wird empfohlen ein Kennwort zu vergeben, da dieser Account standardmäßig der lokalen Administratoren-Gruppe zugewiesen wird.
   b) Eingabe eines Kennworthinweises: Hierbei handelt es sich um eine erforderliche Eingabe für den Fall, dass ein Kennwort vergeben wurde. Es sollte als Erinnerungshilfe für das Kennwort dienen, jedoch nicht gleich dem Kennwort sein.
3. Eingabe des Windows-Produkt Schlüssels: Da Windows 7 als Microsoft Produkt zu aktivieren ist, ist an dieser Stelle der entsprechende Windows-Produktschlüssel anzugeben. Es besteht die Möglichkeit, die Aktivierung automatisch über das Internet durchzuführen. Dazu ist die Option „Windows automatisch aktivieren, wenn eine Internetverbindung besteht“ auszuwählen. Die Eingabe des Windows-Produktschlüssels ist optional und kann auch noch zu einem späteren Zeitpunkt durchgeführt werden.
4. Auswahl des Windows Schutzmechanismus: Für den Schutz des APC sind drei mögliche Windows Schutzmechanismen möglich:

a) Empfohlene Einstellungen verwenden: Damit werden die wichtigsten und von Microsoft empfohlenen Updates automatisch installiert. Weiterhin wird die online Problemlösung von Microsoft genutzt. Es sind keine weiteren Einstellungen notwendig.

b) Nur wichtige Updates installieren: Es werden nur Sicherheitsupdates und andere wichtige Updates (Hot-Fixes oder Patches) für Windows installiert.

c) Später erneut nachfragen: Mit dieser Einstellung werden keine Updates automatisch heruntergeladen und installiert.

5. Einstellung der Zeitzone und der korrekten Uhrzeit: Für den APC sind die Zeit- und die Datumseinstellung vorzunehmen.

   a) Einstellung der Zeitzone: „(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien“ - Aktivierung „Uhr automatisch auf Sommer-/Winterzeit umstellen“,

   b) Einstellung des aktuellen Datums,

   c) Einstellung der aktuellen Uhrzeit.

6. Auswahl des aktuellen Standorts des Computers: Wird eine aktive Netzwerkverbindung erkannt, wird diese einem Netzwerkstandort zugewiesen. Es können verschiedene Netzwerkstandorte definiert und individuelle und spezifische Einstellungen vorgenommen werden. Diese werden dann bei der Erkennung des entsprechenden Netzwerks automatisch angewendet. Es ist zwischen drei möglichen Standorten zu wählen.

   a) Heimnetzwerk: Diese Einstellung sollte bei vertrauenswürdigen Netzwerken genutzt werden.

   b) Arbeitsplatznetzwerk: Diese Einstellung sollte bei Netzwerken angewendet werden, wenn der APC z. B. Mitglied einer Windows-Domäne oder Arbeitsgruppen-Netzwerk ist und dieses Netzwerk vertrauenswürdig ist.

   c) Öffentliches Netzwerk: Diese Einstellung sollte man bei Netzwerken nutzen, die nicht vertrauenswürdig sind oder bei unbekannten Netzwerken.

7. Abschluss der Installation: Persönliche Einstellungen und Desktop Vorbereitungen werden vorgenommen.

3.2.2 Installation via Image

Mit einer Image-Installation wird ein vorbereitetes Systemabbild auf APCs mit identischer Hardware ausgerollt. Dabei werden alle Konfigurationen und Identifikation auf alle APCs angewendet. Man erhält damit eine exakte Kopie eines Betriebssystems auf verschiedenen APCs. Voraussetzung dafür ist die Verwendung identischer Hardware wie z. B. Chipsatz, Grafikkarte, Controller, etc. Die Vorgehensweise für eine Installation mit einem Image ist abhängig vom Hersteller des Image-Programms.

In Abschnitt 5.1 wird die Erstellung eines Images mit Hilfe des Windows-Programms `ImageX.exe` nach erfolgreich durchgeführter Minimierung und Härtung beschrieben. Beim Ausrollen eines Images werden alle Einstellungen auf andere APC übernommen. Dies beinhaltet auch möglicherweise vorhandene Fehler innerhalb eines Images. Daher ist ein Image vor der Durchführung eines Roll-Outs zu testen. Des Weiteren werden alle charakteristischen Merkmale eines APCs wie z. B. UUID, GUID, SID, erster lokaler Benutzername und Passwort, Computername, Lizenzschlüssel etc. durch das Image vorgegeben. Die spezifischen Einstellungen wie z. B. Computername und ggf. Windows-Aktivierungsschlüssel des APC sind daher im Anschluss an die Durchführung eines Roll-Outs noch vorzunehmen.

3.2.3 Installation via Netzwerkverteilung

Windows 7 kann ebenso über den Windows-Bereitstellungsdienst installiert werden. Wenn der APC über eine PXE-bootfähige Netzwerkkarte verfügt, kann mit Hilfe eines Startabbilds der Client über ein Netzwerk gebootet werden. Nach einem erfolgreichen Laden des Startabbilds wird das Installationsabbild gestartet. Ab diesem Zeitpunkt ist der Installationsvorgang identisch wie voran in Abschnitt 3.2.1 beschrieben. Die erste und dritte Installationsphase können durch eine Antwortdatei automatisiert werden. Dabei werden alle notwendigen Eingaben automatisiert an das zu installierende Betriebssystem weitergeleitet. In Abschnitt 5.3 wird die Erstellung einer solchen Antwortdatei beschrieben. Weiterhin kann als Installationsabbild ein minimiertes Referenzsystem hinterlegt werden, das eine grundlegende Absicherung wie z. B. die Entfernung ungenutzter Programmen beinhaltet. Dieses Referenzsystem kann wie gewohnt mit einer angepassten Antwortdatei unbeaufsichtigt installiert werden. Gleichermaßen wird diese Methode auch von Softwareprodukten anderer Herstellern genutzt.

4 Absicherung von Windows 7

Betriebssysteme und Anwendungen sind häufig derart vorkonfiguriert, dass ein weitestgehend reibungsloser und komfortabler Betrieb ermöglicht wird. Sicherheitsaspekte spielen meist eine untergeordnete Rolle. Für einen sicheren Betrieb sind die Standardeinstellungen daher anzupassen.

Grundsätzlich ist bei der Absicherung das Minimalprinzip zu verfolgen. Dies bedeutet, dass alle Softwarebestandteile und Funktionen entfernt werden, die nicht für die vorgesehenen Aufgaben benötigt werden.

Die Betrachtung von Zugriffsrechten und Sicherheitsrichtlinien der lokalen Firewall ist nicht Bestandteil dieser Dokumentation. Hierfür sollten die vorhandenen Richtlinien der Organisation Anwendung finden. Informationen zur Gestaltung des Netzes und zu Zugriffsregelungen von APCs finden sich in [ISi-LANA] und [ISi-Client].

Grundsätzlich sollen:

- Alle Benutzer oder Prozesse nur die Zugriffsberechtigungen erhalten, die sie für ihre Tätigkeiten benötigen. Erweiterte administrative Berechtigungen sollten nur für den Zeitraum vergeben werden, in dem diese administrative Tätigkeiten ausgeführt werden.
- Alle eingehenden Netzwerkverbindungen sollten grundsätzlich verboten werden. Sind bestimmte eingehende Verbindungen erforderlich, so müssen diese explizit freigeschaltet werden. Grundsätzlich ist zu hinterfragen, ob auf einem APC ein Dienst für Dritte gestartet werden sollte. Dies ist normalerweise die Aufgabe eines Netzwerkservers.
  Achtung: Einige Anwendungen und Dienste erstellen eine automatisch generierte Freischaltung in der Regelliste. Diese sind grundsätzlich auf Ihre Notwendigkeit hin zu überprüfen.

Die Absicherung erfolgt in drei Schritten:

1. Deaktivierung nicht erforderlicher Komponenten (Abschnitt 4.1)
2. Konfiguration der verbleibenden Komponenten (Abschnitt 4.2)
3. Konfiguration der Betriebssystemdienste (Abschnitt 4.3)

Der folgende Absatz erläutert kurz die Vorgehensweise bei Minimierung und Absicherung, sowie deren Darstellung in diesem Dokument.

Vorgehensweise bei der Absicherung

Vor Änderungen am APC sollte eine Sicherung der Registrierungsdatenbank durchgeführt werden (siehe Abschnitt 2.2.5). Im Falle einer fehlerhaften Konfiguration ermöglicht dies eine schnelle und einfache Wiederherstellung des Systems.

Für die Durchführung der Absicherung des APCs werden die folgenden administrativen Werkzeuge eingesetzt:

Werkzeug	*Symbol*
Grafische Benutzeroberfläche GUI (*Graphical User Interface*)	
Registrierungsdatenbank Registry	
Gruppenrichtlinien GPO (*Group Policy Object)*	

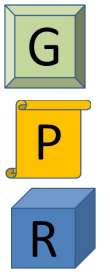
Tabelle 14: Übersicht der Konfigurationswerkzeuge

Die in Tabelle 14 aufgeführten Symbole werden im Folgenden am linken Seitenrand positioniert. Dadurch lässt sich der angegebene Konfigurationsschritt einem Werkzeug zuordnen.

Sind für die Konfiguration einer Funktion mehrere Schritte notwendig, so werden diese durch eine Trennlinie am linken Seitenrand separiert. Für jeden einzelnen Schritt werden immer alle möglichen Werkzeuge aufgeführt. Da die verschiedenen Konfigurationswerkzeuge nicht alle gleich mächtig sind, kommt es vor, dass einige Konfigurationsschritte nur mit bestimmten Werkzeugen möglich sind. Sind mehrere Werkzeuge aufgeführt, so kann der Administrator ein beliebiges dieser Werkzeuge wählen.

Es sind grundsätzlich alle Teilschritte durchzuführen.

Im nachfolgenden Beispiel sind zwei Konfigurationsschritte durchzuführen, wobei sich der erste Schritt mit allen drei Werkzeugen (GUI, GPO, Registry) durchführen lässt. Der zweite Schritt ist nur über die Registry möglich.



Der erste Konfigurationsschritt kann über die Werkzeuge GUI, GPO und Registry vorgenommen werden. Der Administrator kann sich für eine der drei Möglichkeiten entscheiden.

Der zweite Konfigurationsschritt kann nur über das Werkzeug Registry vorgenommen werden. Der Administrator muss dieses Werkzeug verwenden.

4.1 Deaktivierung von Betriebssystemkomponenten

Nachfolgend werden die notwendig durchzuführenden Schritte zur Deaktivierung verschiedener Betriebssystemkomponenten beschrieben. Es wird darauf hingewiesen, dass die beschriebenen Änderungen sich auf die für die Untersuchung definierten Standard-Anwendungen beziehen.

4.1.1 Deaktivieren von Netzwerkelementen

Bei der Standardinstallation von Windows 7 werden bei einer aktiven Netzwerkkarte folgende Elemente automatisch installiert:

- Client für Microsoft - (Netzwerk-Client)
- QoS-Paketplaner - (Netzwerk-Dienst)
- Datei- und Druckerfreigabe für Microsoft-Netzwerke - (Netzwerk-Dienst)
- Internetprotokoll Version 6 (TCP/IPv6) - (Netzwerk-Protokoll)
- Internetprotokoll Version 4 (TCP/IPv4) - (Netzwerk-Protokoll)
- E/A-Treiber für Verbindungsschicht-Topologieerkennung - (Netzwerk-Protokoll)
- Antwort für Verbindungsschicht-Topologieerkennung - (Netzwerk-Protokoll)

Für die Standard-Anwendungen eines APC reichen der Netzwerk-Client „Client für Microsoft“ sowie die Netzwerk-Protokolle „Internetprotokoll Version 4 (TCP/IPv4)“ und/oder „Internet-protokoll Version 6 (TCP/IPv6)“ als Single- oder Dual-Stack-Betrieb. Je nach gewünschtem Protokoll müssen die entsprechenden Komponenten aktiviert werden. Der nachfolgende Screenshot ist also nur als Beispiel zu sehen. Werden zusätzliche Dienste des Clients in der Infrastruktur benötigt, so sind diese vorher mit den Verantwortlichen für den Bereich Netzwerk abzustimmen.

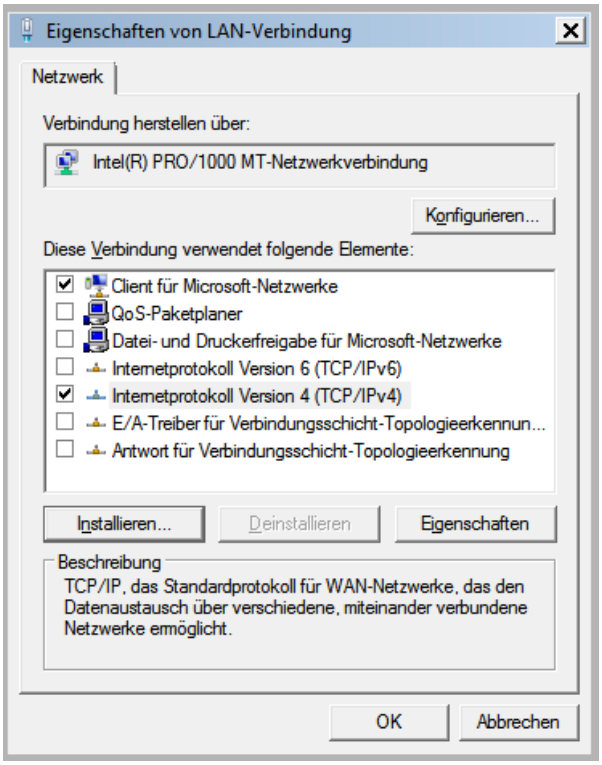


Abbildung 4.1: Die Eigenschaften der LAN-Verbindung

Start → Systemsteuerung → Netzwerk- und Freigabecenter → Adaptereinstellungen ändern → LAN-Verbindung → Eigenschaften

Default-Wert	Client für Microsoft-Netzwerke QoS-Paketplaner Datei- und Druckerfreigabe für Microsoft-Netzwerke Internetprotokoll Version 4 (TCP/IPv4) Internetprotokoll Version 6 (TCP/IPv6) E/A-Treiber für Verbindungsschicht-Topologieerkennung Antwort für Verbindungsschicht-Topologieerkennung
Neuer Wert	Client für Microsoft-Netzwerke Internetprotokoll Version 4 (TCP/IPv4) und/oder Internetprotokoll Version 6 (TCP/IPv6)

Folgender Schritt dient der Deaktivierung von IPv6-Tunneln:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters[69]
Neuer DWORD-Wert (32-bit): *DisabledComponents*

Default-Wert	Nicht vorhanden
Neuer Wert	0x01

4.1.2 Deinstallation von Windows-Funktionen

Bei der Erstinstallation von Windows 7 werden einige Anwendungen automatisch installiert. Die hiermit bereitgestellten Funktionen sind wie nachfolgend beschrieben, zu deaktivieren. Nach der Deinstallation der beschriebenen Komponenten verbleiben noch vier Windows-Funktionen.

1. Medienfunktionen (Windows Media Player)
2. Microsoft .NET Framework 3.5.1
3. Windows Search
4. Microsoft Internet Explorer 8

69 http://support.microsoft.com/kb/929852

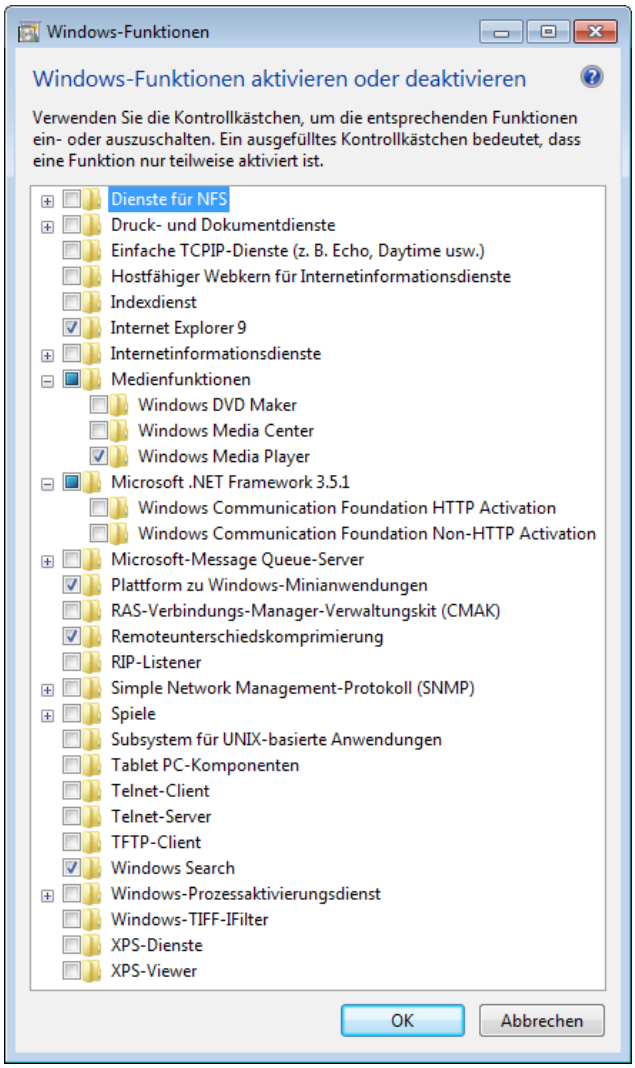


Abbildung 4.2: Deaktivierung von Windows-Funktionen

G

Start → Systemsteuerung → Programme und Funktionen → Windows-Funktionen aktivieren oder deaktivieren

Default-Wert	Druck- und Dokumentdienste (Internetdruckclient, Windows Fax und -Scan) Internetinformationsdienste (WWW-Dienste, Gemeinsam genutzte HTTP-Features, Sicherheit) Medienfunktionen Microsoft .NET Framework 3.5.1 Plattform zu Windows-Minianwendungen Remoteunterschiedskomprimierung Windows Search Windows-Prozessaktivierungsdienst XPS-Dienste XPS-Viewer
Neuer Wert	Medienfunktionen (Windows Media Player) Microsoft .NET Framework 3.5.1

Default-Wert	Druck- und Dokumentdienste (Internetdruckclient, Windows Fax und -Scan) Internetinformationsdienste (WWW-Dienste, Gemeinsam genutzte HTTP-Features, Sicherheit) Medienfunktionen Microsoft .NET Framework 3.5.1 Plattform zu Windows-Minianwendungen Remoteunterschiedskomprimierung Windows Search Windows-Prozessaktivierungsdienst XPS-Dienste XPS-Viewer
	Windows Search Internet Explorer 8

4.1.3 Konfiguration der Startprogramme

Einige Programme hinterlegen in der Registry einen Autostartmechanismus.[70] Diese Programme werden im Hintergrund gestartet, selbst wenn sie aktuell nicht benötigt werden. In diesem Abschnitt werden die Autostarteinstellungen überprüft.

G

Start → Ausführen → `msconfig.exe` → Rechtsklick → „Als Administrator ausführen“ → Allgemein

Default-Wert	Normaler Systemstart
Neuer Wert	Benutzerdefinierter Systemstart (Systemdienste laden, Systemstartelemente laden)

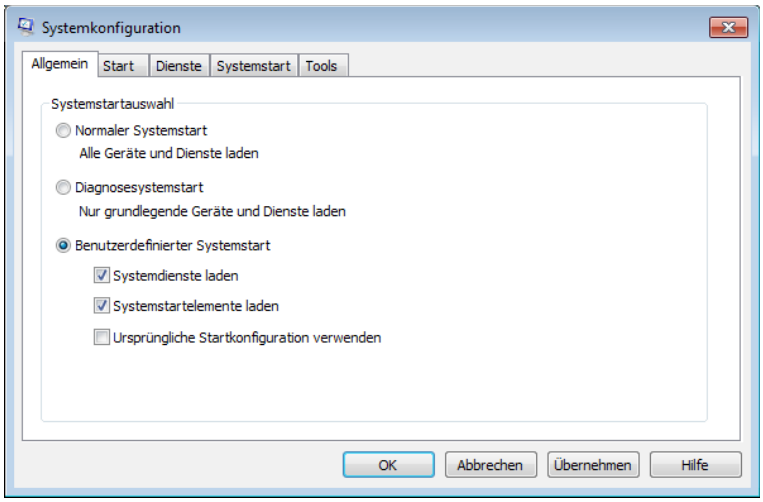


Abbildung 4.3: Systemkonfiguration, Allgemeine Einstellungen

G

Start → Ausführen → `msconfig.exe` → Rechtsklick → „Als Administrator ausführen“ → Start

Default-Wert	Keine Startoption gewählt
Neuer Wert	Kein GUI-Start

70 http://technet.microsoft.com/en-us/magazine/ee851671.aspx

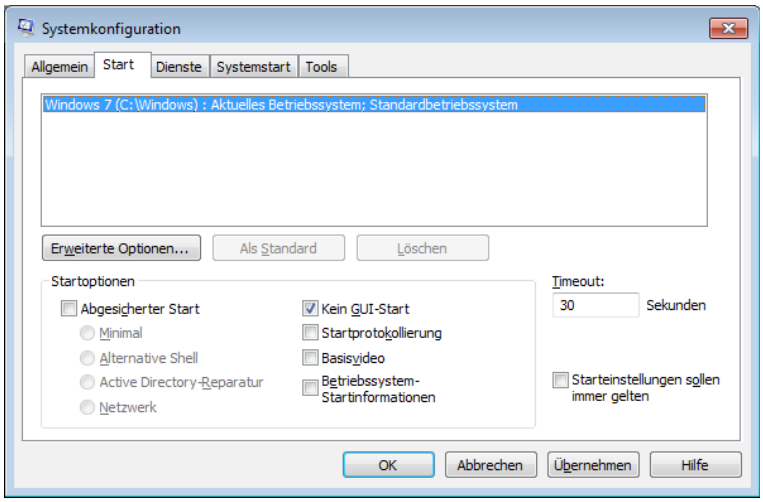


Abbildung 4.4: Systemkonfiguration, Start Einstellungen

G

Start → Ausführen → `msconfig.exe` → Rechtsklick → „Als Administrator ausführen“ → Systemstart

Default-Wert	Keine Auswahl
Neuer Wert	Systemstartelemente deaktivieren, die nicht gestartet werden sollen

R

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Default-Wert	Eingetragene Software zum Autostart
Neuer Wert	Entsprechende Schlüssel entfernen

R

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`

Default-Wert	Eingetragene Maschinengebundene Software zum einmaligen Autostart
Neuer Wert	Entsprechende Schlüssel entfernen

R

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WoW6432Node\Microsoft\Windows\CurrentVersion\Run`

Default-Wert	Eingetragene Maschinengebundene Software zum einmaligen Autostart
Neuer Wert	Entsprechende Schlüssel entfernen

R

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WoW6432Node\Microsoft\Windows\CurrentVersion\RunOnce`

Default-Wert	Eingetragene Maschinengebundene Software zum einmaligen Autostart
Neuer Wert	Entsprechende Schlüssel entfernen

R

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Default-Wert	Benutzergebundene Software zum Autostart aller Benutzer
Neuer Wert	Entsprechende Schlüssel entfernen

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Run`

Default-Wert	Benutzergebundene Software zum Autostart aller Benutzer
Neuer Wert	Entsprechende Schlüssel entfernen

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows`

Default-Wert	Benutzergebundene Software zum Autostart aller Benutzer
Neuer Wert	Entsprechende Schlüssel entfernen

4.1.4 Deinstallation von Windows-Minianwendungen

Windows-Minianwendungen sind standardmäßig installiert, können aber vom APC entfernt werden, um die Angriffsfläche zu verringern.

Abbildung 4.5: Deinstallation von Windows-Minianwendungen

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Desktopkminianwendungen → Desktopkminianwendungen deaktivieren

Default-Wert	nicht konfiguriert
Neuer Wert	Aktiviert

Start → Systemsteuerung (Ansicht: Kategorie) → Programme → Minianwendung deinstallieren → Minianwendung mit Rechtsklick auswählen → Deinstallieren auswählen

Default-Wert	-
Neuer Wert	Alle Minianwendungen deaktivieren

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Windows\`
Neuer Schlüssel: *Sidebar*
Neuer DWORD-Wert (32-bit): *TurnOffSidebar*

Default-Wert	Nicht konfiguriert
Neuer Wert	1

4.1.5 Deaktivierung Windows Messenger

Der Windows Messenger[71] ist eine Anwendung zur schnellen Kommunikation mit anderen Nutzern. In diesem Abschnitt wird der nicht benötigte Windows Messenger deaktiviert.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Windows Messenger → Windows Messenger nicht automatisch starten

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\`
Neuer Schlüssel: *Messenger\Client*
Neuer DWORD-Wert (32-bit): *PreventAutoRun*

Default-Wert	Nicht vorhanden
Neuer Wert	1

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Windows Messenger → Ausführung von Windows Messenger nicht zulassen

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\`
Neuer Schlüssel: *Messenger\Client*
Neuer DWORD-Wert (32-bit): *PreventRun*

Default-Wert	Nicht vorhanden
Neuer Wert	1

4.1.6 Deaktivierung Windows Mail

Windows Mail[72] ist die integrierte E-Mail-Anwendung. Da ein separates Programm für E-Mail und Kalender verwendet wird, kann Windows Mail deaktiviert werden.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Windows Mail → Windows Mail-Anwendung deaktivieren

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\`
Neuer Schlüssel: *Windows Mail*

71 http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=14788
72 http://windows.microsoft.com/en-US/windows7/looking-for-windows-mail

Neuer DWORD-Wert (32-bit): *ManualLaunchAllowed*

Default-Wert	Nicht vorhanden
Neuer Wert	0

4.1.7 Deaktivierung Spiel-Explorer

Der Spiele-Explorer[73] stellt Anwendungen zur Unterhaltung bereit. Diese Anwendungen werden nicht genutzt und werden daher in diesem Abschnitt deaktiviert.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Spiel-Explorer → Herunterladen von Spielinformationen deaktivieren

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows`
Neuer Schlüssel: *GameUX*
Neuer DWORD-Wert (32-bit): *DownloadGameInfo*

Default-Wert	Nicht vorhanden
Neuer Wert	0

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Spiel-Explorer → Spielupdates deaktivieren

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows`
Neuer Schlüssel: *GameUX*
Neuer DWORD-Wert (32-bit): *GameUpdateOptions*

Default-Wert	Nicht vorhanden
Neuer Wert	0

4.1.8 Deaktivierung Windows-Mobilitätscenter

Das Windows Mobilitätscenters[74] stellt Anwendungen zur Steuerung von mobilen APCs bereit. Da der hier betrachtete APC ein Desktop-System ist, kann diese Anwendung deaktiviert werden.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Windows-Mobilitätscenter → Windows-Mobilitätscenter deaktivieren

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies`

73 http://windows.microsoft.com/en-US/windows7/products/features/games-explorer
74 http://windows.microsoft.com/en-US/windows-vista/Using-Windows-Mobility-Center

Neuer Schlüssel: *MobilityCenter*
Neuer DWORD-Wert (32-bit): *NoMobilityCenter*

Default-Wert	Nicht vorhanden
Neuer Wert	1

4.1.9 Deaktivierung Digitalschließfach

Das digitale Schließfach dient zur Bereitstellung von Anwendungen im Windows Marketplace[75]. Diese Funktion wird für den im Rahmen dieser Anleitung betrachteten APC nicht benötigt und wird daher deaktiviert.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → Digitalschließfach → Digitalschließfach nicht ausführen

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Digital Locker`
Neuer Schlüssel: *MobilityCenter*
Neuer DWORD-Wert (32-bit): *DoNotRunDigitalLocker*

Default-Wert	Nicht vorhanden
Neuer Wert	1

4.1.10 Deaktivierung Remoteshell

Die Remoteshell[76] dient zur Fernwartung von APCs mittels Kommandozeile. Diese Funktion wird für den im Rahmen dieser Anleitung betrachteten APC nicht benötigt und wird daher deaktiviert.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → Windows-Remoteshell → Remoteshellzugriff zulassen

Default-Wert	Nicht konfiguriert
Neuer Wert	Deaktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\`
Neuer Schlüssel: *WinRM/Service/WinRS*
Neuer DWORD-Wert (32-bit): *AllowRemoteShellAccess*

Default-Wert	Nicht vorhanden
Neuer Wert	0

4.1.11 Deaktivierung des Remotedesktop

Der Remotedesktop[77] dient zur Fernwartung von APCs mittels Anzeige des Bildschirms. Soll innerhalb einer Windows Domäne die Fernwartung mittels Remotedesktop genutzt werden, so ist der Zugriff wie folgt abzusichern:

75 http://www.windowsmarketplace.com/
76 http://technet.microsoft.com/en-us/library/cc785056(WS.10).aspx
77 http://windows.microsoft.com/en-US/windows7/Remote-Desktop-Connection-frequently-asked-questions

Start → Systemsteuerung → System → Remoteeinstellungen → Remote → Remotedesktop→ Benutzerauswahl

Default-Wert	Keine Verbindung mit diesem Computer zulassen
Neuer Wert	Verbindungen nur von Computern zulassen, auf denen Remotdesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird (höhere Sicherheit)[78]

Soll keine Fernwartung hierüber zugelassen werden, kann Remotedesktop abgeschaltet werden.

Start → Systemsteuerung → System → Remoteeinstellungen → Remote → Remotedesktop

Default-Wert	Keine Verbindung mit diesem Computer zulassen.
Neuer Wert	Keine Verbindung mit diesem Computer zulassen.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\fDenyConnections`

Default-Wert	0
Neuer Wert	1

4.1.12 Deaktivierung der Remoteunterstützung

Die Remoteunterstützung[79] wird zur Hilfestellung von Dritten verwendet und kann deaktiviert werden.

Start → Systemsteuerung → System → Remoteeinstellungen → Remote → Remoteunterstützung → Remoteunterstützungsverbindung mit diesem Computer zulassen

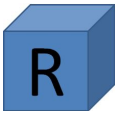
Default-Wert	Aktiviert
Neuer Wert	Deaktiviert

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Remote Assistance\fAllowToGetHelp`

Default-Wert	1
Neuer Wert	0

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → System → Remoteunterstützung → Angeforderte Remoteunterstützung

Default-Wert	Nicht konfiguriert
Neuer Wert	Deaktiviert



`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\`
Neuer Schlüssel: *Terminal Services*
Neuer DWORD-Wert (32-bit): *fAllowToGetHelp*

78 http://support.microsoft.com/kb/951608/
79 http://windows.microsoft.com/en-US/windows-vista/What-is-Windows-Remote-Assistance

Default-Wert	Nicht vorhanden
Neuer Wert	0

4.1.13 Deaktivierung von Dateifreigabe über Windows Media Player

Zur Unterbindung der Dateifreigabe[80] mittels des Windows Media Players wird diese Funktion hier deaktiviert. Bei einer aktiven Dateifreigabe könnten Daten von Dritten eingesehen werden. Daher ist diese Funktion zu deaktivieren.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → Windows Media Player → Medienfreigabe verhindern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\`
Neuer Schlüssel: *WindowsMediaPlayer*
Neuer DWORD-Wert (32-bit): *PreventLibrarySharing*

Default-Wert	Nicht vorhanden
Neuer Wert	1

4.1.14 Autostart deaktivieren

In diesem Abschnitt wird das automatische Starten von Programmen von Datenträgern deaktiviert.

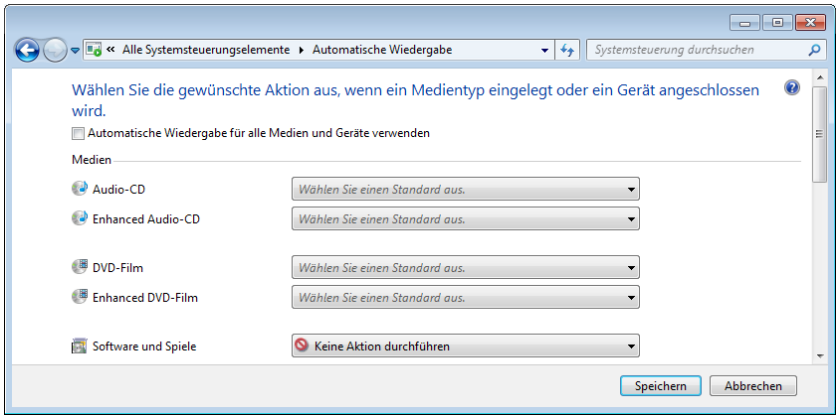


Abbildung 4.6: Konfiguration der Automatischen Wiedergabe

Start → Systemsteuerung → Automatische Wiedergabe

Default-Wert	Automatische Wiedergabe für alle Medien und Geräte verwenden → Aktiviert
Neuer Wert	Automatische Wiedergabe für alle Medien und Geräte verwenden → Deaktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\`
Neues REG_DWORD:
Name: NoDriveTypeAutoRun

80 http://windows.microsoft.com/de-DE/windows-vista/Sharing-media-on-a-network-using-Windows-Media-Player

Default-Wert	Nicht vorhanden
Neuer Wert	FF

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → Richtlinien für die automatische Wiedergabe → Autoplay deaktivieren

Default-Wert	nicht konfiguriert
Neuer Wert	Aktiviert → Alle Laufwerke

4.1.15 Deaktivierung von ActiveX

Wird dieser Schalter aktiviert, werden nur signierte Active-X Steuerelemente installiert.

Anmerkung: Die Verwendung der GPO ist bei dieser Konfiguration vorzuziehen, da dies die Härtung vereinfacht.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → ActiveX-Installerdienst → ActiveX-Installationsrichtlinie für Sites in vertrauenswürdigen Zonen

Optionen: Benutzer zur Eingabe auffordern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Anmerkung: Die GPO legt Schlüssel unter den folgenden Registrierungspfaden an:
`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{%Wert%}Machine\SOFTWARE\Policies\Microsoft\Windows\AxInstaller\AxISURLZonePolicies`
`HKEY_USERS\S-1-5-21-%Wert%\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{%Wert%}Machine\SOFTWARE\Policies\Microsoft\Windows\AxInstaller`

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\`
Neuer Schlüssel: `AxInstaller`
Neuer Unterschlüssel: *AxISURLZonePolicies*
Neuer DWORD-Wert (32-bit): *IgnoreInvalidCertDate*
Neuer DWORD-Wert (32-bit): *IgnoreInvalidCN*
Neuer DWORD-Wert (32-bit): *IgnoreUnknownCA*
Neuer DWORD-Wert (32-bit): *IgnoreWrongCertUsage*
Neuer DWORD-Wert (32-bit): *InstallSignedOCX*
Neuer DWORD-Wert (32-bit): *InstallTrustedOCX*
Neuer DWORD-Wert (32-bit): *InstallUnSignedOCX*

Default-Wert	Nicht vorhanden
Neuer Wert	0 / 0 / 0 / 0 / 1 / 1 / 1

4.1.16 Deaktivierung von Windows Anytime Upgrade

Damit die Windows 7 Edition nicht verändert werden kann, wird in diesem Abschnitt Windows Anytime[81] abgeschaltet. Somit werden alle auf Windows 7 basierenden APCs auf dem gleichen Versionsstand gehalten.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Windows Komponenten → Windows Anytime Upgrade → Ausführung von Windows Anytime Upgrade verhindern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\WAU`
Neues REG_DWORD:
Name: Disabled

Default-Wert	Nicht vorhanden
Neuer Wert	1

4.1.17 Verhinderung einer Internetinformationsdienste (IIS) Installation

Um die Installation des IIS auf dem APC zu verhindern, sind die folgenden Einstellungen durchzuführen.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → Internetinformationsdienste → IIS-Installation verhindern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\`
Neuer Schlüssel: *IIS*
Neuer DWORD-Wert (32-bit): *PreventISSInstall*

Default-Wert	Nicht vorhanden
Neuer Wert	1

4.1.18 Deaktivierung von NetMeeting Freigaben

Zur Verhinderung von NetMeeting Freigaben des APC ist diese Funktion wie nachstehend beschrieben zu deaktivieren.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → NetMeeting → Remotedesktop-Freigabe deaktivieren

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\`

81 http://windows.microsoft.com/en-US/windows7/products/features/windows-anytime-upgrade

Neuer Schlüssel: *Conferencing*
Neuer DWORD-Wert (32-bit): *NoRDS*

Default-Wert	Nicht vorhanden
Neuer Wert	1

4.2 Konfiguration von benötigten Betriebssystemkomponenten

Dieser Abschnitt geht auf die Konfiguration der Windows-Komponenten ein, die nicht deinstalliert oder deaktiviert wurden.

4.2.1 Windows Defender

Windows Defender[82] ist eine Spyware-Schutzsoftware von Microsoft, die bereits im Funktionsumfang von Windows 7 enthalten ist. Im Enterprise Umfeld wird der Windows Defender häufig durch ein Produkt eines Drittherstellers ersetzt. Virenschutzprogramme anderer Hersteller deaktivieren in der Regel den Windows Defender, um Komplikationen zu vermeiden.

Soll der Windows Defender verwendet werden, lässt er sich über die Schaltfläche Start → Systemsteuerung → Windows Defender wie folgt konfigurieren. Der Windows Defender benötigt den gleichnamigen System-Dienst. Dieser darf bei einer Verwendung des Windows Defenders nicht wie in Abschnitt beschrieben, deaktiviert werden.

Start → Systemsteuerung → Windows Defender → Extras → Optionen → Standardaktionen

Default-Wert	Empfohlene Aktion basierend auf Definitionen
Neuer Wert	Alle Elemente auf Quarantäne, Empfohlene Aktionen anwenden

Start → Systemsteuerung → Windows Defender → Extras → Optionen → Erweitert

Default-Wert	E-Mail überprüfen deaktiviert, Wechseldatenträger überprüfen deaktiviert
Neuer Wert	Aktionen aktivieren

Start → Systemsteuerung → Windows Defender → Extras → Unter Quarantäne → Microsoft SpyNet beitreten

Default-Wert	Als Premiummitglied beitreten
Neuer Wert	Microsoft Spynet jetzt nicht beitreten

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\SpyNet\`
Neues REG_DWORD:
Name: SpyNetReporting

Default-Wert	Nicht vorhanden
Neuer Wert	0

82 http://www.microsoft.com/germany/windows/products/winfamily/defender/default.mspx

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Windows Defender → Microsoft SpyNet-Berichterstattung konfigurieren

Default-Wert	nicht konfiguriert
Neuer Wert	Deaktiviert

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Windows Defender → Vor geplanten Scanvorgängen auf neue Signaturen überprüfen

Default-Wert	nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Scan\`

Neuer REG_DWORD
Name: CheckForSignaturesBeforeRunningScan

Default-Wert	Nicht vorhanden
Neuer Wert	1

4.2.2 Konfiguration der Anmeldeinformationen

Dieser Schalter trägt dazu bei, dass Anmeldeinformatioen ein vertrauenswürdiger Pfad verwenden, was das Abhören des Benutzerkennwortes für Windows durch Schadprogramme erschwert.

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Benutzerschnittstelle für Anmeldeinformationen → Vertrauenswürdiger Pfad für Anmeldeinformationseintrag erforderlich

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\`
Neuer Schlüssel: *CredUI*
Neuer DWORD-Wert (32-bit): *EnableSecureCredentialPrompting*

Default-Wert	Nicht vorhanden
Neuer Wert	1

4.2.3 Aktivierung von SEHOP

Die Structured Exception Handling Overwrite Protection (SEHOP) ist ein bereits in Windows 7 integrierter Schutz gegen Angriffe über die Überschreibenfunktion des Ausnahmehandlers SEH[83]. Bei einigen Anwendungen kann SEHOP zu Fehlern führen. Daher müssen Anwendungen vorab mit dieser Einstellung getestet werden.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\kernel`
Neues REG_DWORD:
Name: DisableExceptionChainValidation

83 http://support.microsoft.com/kb/956607/de

Default-Wert	Nicht vorhanden
Neuer Wert	0

4.2.4 Aktivierung von No-Execute Bit (NX-Bit) – Die Datenausführungsverhinderung

Hier wird das No-Execute Bit zur Aktivierung der *Datenausführungsverhinderung* gesetzt (siehe auch Abschnitt 2.3.3).

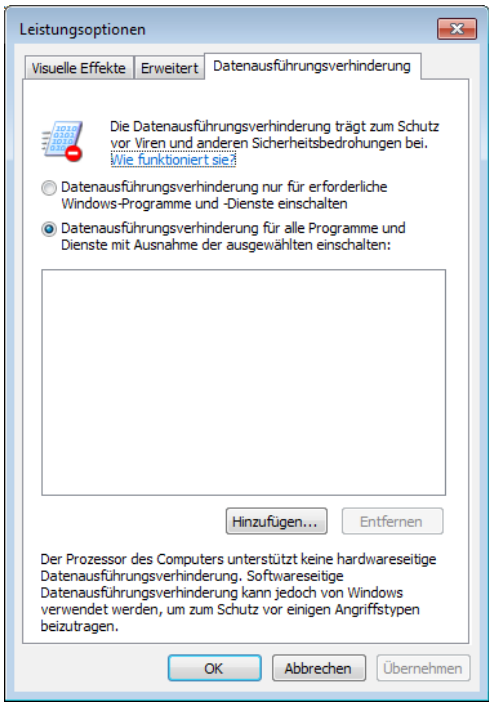


Abbildung 4.7: Aktivierung der Datenausführungsverhinderung

Start → Systemsteuerung → System → Erweiterte Systemeinstellungen → Erweitert → Einstellungen von Leistung → Datenausführungsverhinderung

Default-Wert	Datenausführungsverhinderung nur für erforderliche Windows-Programme und -Dienste einschalten
Neuer Wert	Datenausführungsverhinderung für alle Programme und Dienste mit Ausnahme der ausgewählten einschalten

4.2.5 Windows Firewall Konfiguration

Die im Microsoft Windows 7 Funktionsumfang beinhaltete Firewall ist zu konfigurieren über Systemsteuerung / Verwaltung / Windows Firewall mit erweiterter Sicherheit / Rechts-Klick auf Windows Firewall mit erweiterter Sicherheit → Eigenschaften.

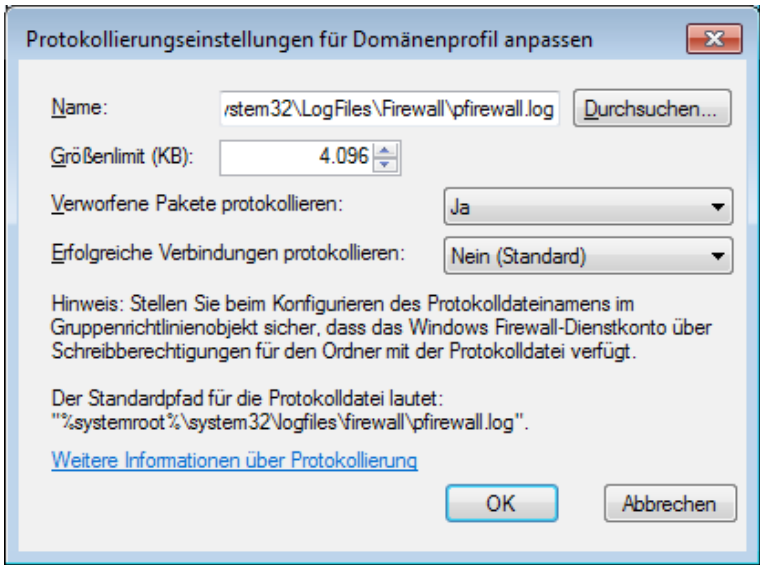


Abbildung 4.8: Anpassen der Protokollierungseinstellungen

G

Start → Systemsteuerung → Verwaltung → Windows Firewall mit erweiterter Sicherheit → Rechts-Klick auf Windows Firewall mit erweiterter Sicherheit → Eigenschaften → Auswahl des Profils → unter Protokollierung → Anpassen → Verworfene Pakete protokollieren

Default-Wert	Nein
Neuer Wert	Ja

R

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\Logging\LogDroppedPackets`

Default-Wert	0
Neuer Wert	1

R

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\PublicProfile\Logging\LogDroppedPackets`

Default-Wert	0
Neuer Wert	1

R

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\Logging\LogDroppedPackets`

Default-Wert	0
Neuer Wert	1

P

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Windows Einstellungen → Sicherheitseinstellungen → Windows-Firewall mit erweiterter Sicherheit → Windows-Firewall mit erweiterter Sicherheit - Lokales Gruppenrichtlinienobjekt → Windows-Firewalleigenschaften → Profilauswahl → Protokollierung → Anpassen → Verworfene Pakete Protokollieren

Default-Wert	nicht konfiguriert
Neuer Wert	Konfiguration wie GUI

4.2.6 Windows Update-Manager

Der Windows Update-Manager sorgt für eine angemessene Aktualisierung des APCs.

Im Enterprise-Umfeld ist der Betrieb eines eigenen Update-Servers üblich, der die Aktualisierungen vom Hersteller bezieht und dann die Verteilung an die APCs übernimmt. Informationen zu Update-Servern und dem Verfahren zum Testen und Ausrollen von Updates finden sich in [ISi-Client].

Nachfolgend ist die vorzunehmende Konfiguration des Windows Update-Managers beschrieben.

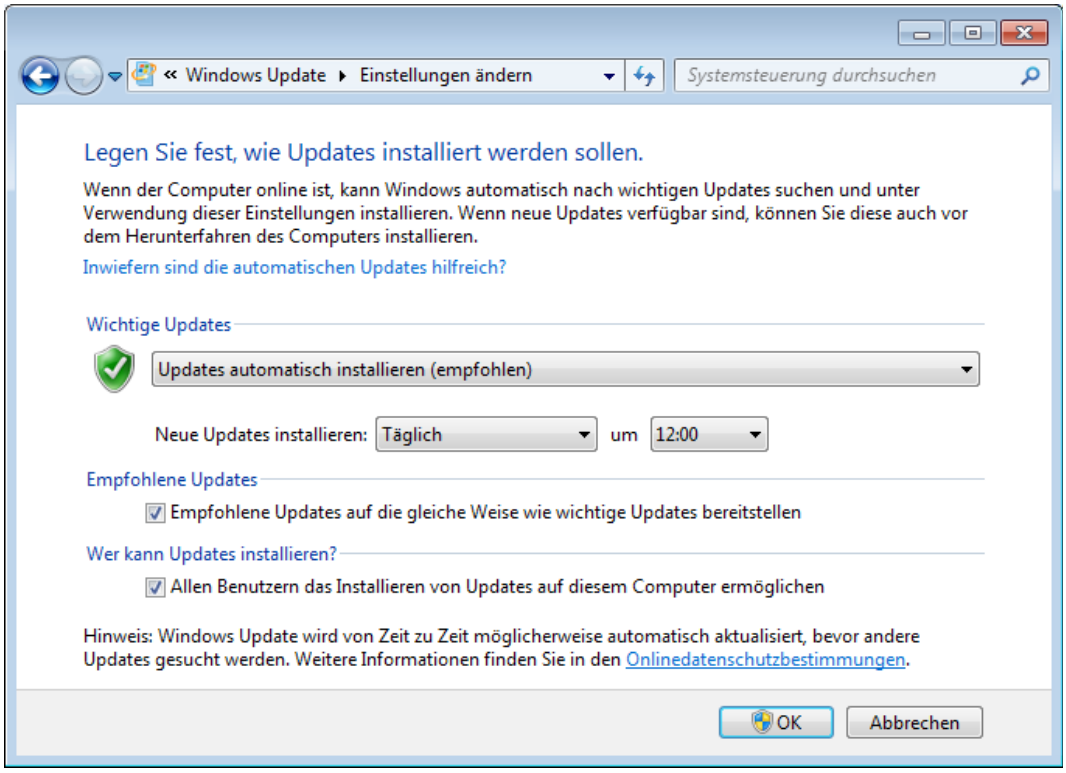


Abbildung 4.9: Einstellungen zum Windows Update

Start → Systemsteuerung → Windows Update → Einstellungen ändern

Default-Wert	Neue Updates automatisch installieren (empfohlen)
Neuer Wert	Neue Updates automatisch installieren (empfohlen)

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → Windows-Komponenten → Windows Update → Automatische Updates konfigurieren

Default-Wert	Nicht konfiguriert
Neuer Wert	4 – Automatisch Herunterladen und laut Zeitplan installieren

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\AUOptions`

Default-Wert	4
Neuer Wert	4

4.2.7 Ausführungskontrolle

Mit einer Ausführungskontrolle lässt sich der Zugriffe auf Anwendungen steuern. In den Versionen Enterprise und Ultimate ist der sog. AppLocker[84] enthalten, dessen Konfiguration nachfolgend beschrieben wird.

Alternativ zum AppLocker lassen sich auch Blacklists oder besser Whitelists verwenden. Relevante Gruppenrichtlinien sind z. B.:

- Benutzerkonfiguration | Administrative Vorlagen | System | Nur zugelassene Windows-Anwendungen ausführen
- Computerkonfiguration | Windows Einstellungen | Sicherheitseinstellungen | Richtlinien für die Softwareeinschränkungen | Sicherheitsstufen | Die Software wird trotz der Berechtigung des Benutzers nicht ausgeführt
- Computerkonfiguration | Windows Einstellungen | Sicherheitseinstellungen | Richtlinien für die Softwareeinschränkungen | zusätzliche Regeln
- Computerkonfiguration | Windows Einstellungen | Sicherheitseinstellungen | Richtlinien für Softwareeinschränkungen | Erzwingen
- Computerkonfiguration | Windows Einstellungen | Sicherheitseinstellungen | Richtlinien für die Softwareeinschränkungen | zusätzliche Regeln

Die Einstellungen zum AppLocker finden sich in der GPO unter folgendem Pfad : Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Windows Einstellungen → Sicherheitseinstellungen → Anwendungssteuerungsrichtlinie → AppLocker

84 http://www.microsoft.com/windows/enterprise/products/windows-7/features.aspx#applocker

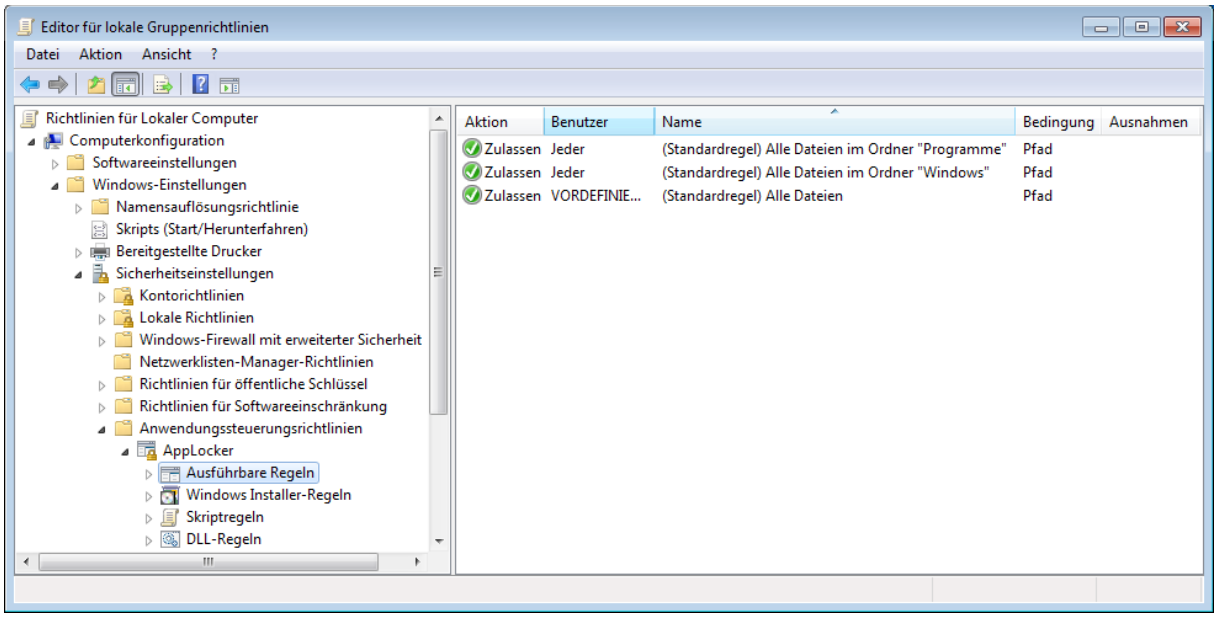


Abbildung 4.10: Konfiguration des AppLocker

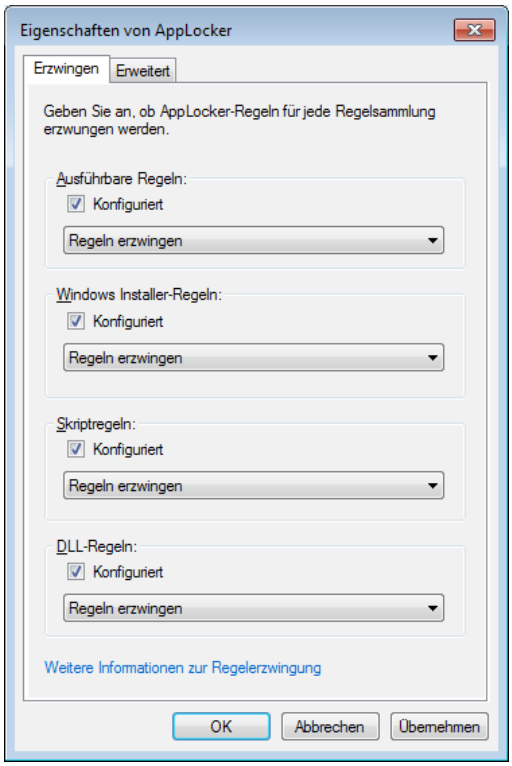


Abbildung 4.11: Eigenschaften des AppLockerc

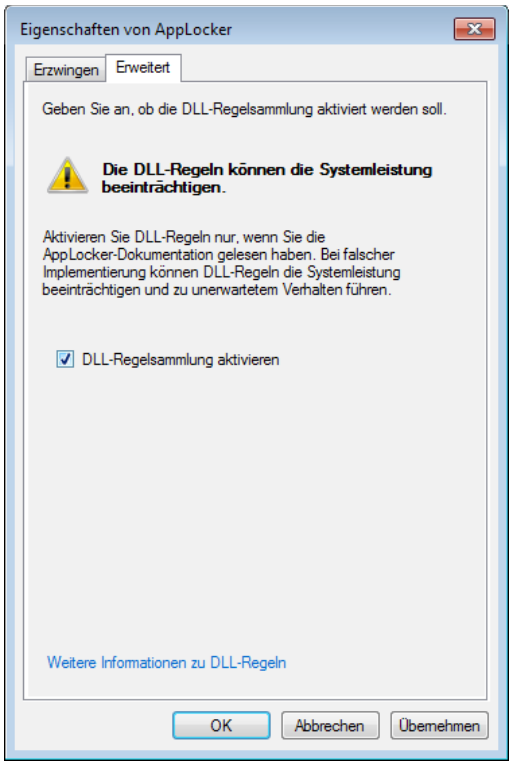


Abbildung 4.12: Erweiterte Eigenschaften des AppLocker

Rechtsklick → Ausführbare Regeln → Aktion → Standardregeln erstellen

Default-Wert	Keine Regel
Neuer Wert	Zulassen / Jeder / Alle Dateien im Ordner Programme Zulassen / Jeder / Alle Dateien im Ordner Windows / Ausnahme / %SYSTEMDRIVE%\Windows\winsxs* Zulassen / Administratoren / Alle Dateien

Rechtsklick → Windows Installer-Regeln → Aktion → Standardregeln erstellen

Default-Wert	Keine Regel
Neuer Wert	Verweigern / Jeder / Alle digital singnierten Windows Installer Dateien Verweigern / Jeder / Alle Windows Installer Dateien unter %SYSTEMDRIVE %\Windows\Installer Zulassen / Administratoren / Alle Windows Installer Dateien

Rechtsklick → Skriptregeln → Aktion → Standardregeln erstellen

Default-Wert	Keine Regel
Neuer Wert	Verweigern / Jeder / alle Scripte im Ordner Programme Verweigern / Jeder / alle Scripte im Ordner Windows Zulassen / Administratoren / Alle Scripte

Eigenschaften von AppLocker

Default-Wert	Keine Regel aktiviert
Neuer Wert	Ausführbare Regeln / Konfiguriert Windows Installer-Regeln / Konfiguriert Scriptregeln / Konfiguriert

Eigenschaften von AppLocker → Erweitert

Default-Wert	DLL-Regelsammlung aktivieren → deaktiviert
Neuer Wert	DLL-Regelsammlung aktivieren → aktiviert

Eigenschaften von AppLocker → Erzwingen

Default-Wert	Keine Regel aktiviert
Neuer Wert	Ausführbare Regeln / Konfiguriert – Regeln erzwingen Windows Installer-Regeln / Konfiguriert – Regeln erzwingen Scriptregeln / Konfiguriert – Regeln erzwingen DLL-Regeln / Konfiguriert – Nur überwachen

Rechtsklick → DLL Regeln → Aktion → Standardregeln erstellen

Default-Wert	Keine Regel
Neuer Wert	Zulassen / Jeder / Microsoft Windows DLLs Zulassen / Jeder / alle DLLs im Ordner Programme

Default-Wert	Keine Regel
	Zulassen / Administrator / Alle DLLs

4.2.8 Beschreibung des Einsatzes der Gerätekontrolle

Die Gerätekontrolle steuert den Zugriff auf extern angeschlossene Geräte, wie USB-Sticks, PDAs, etc. Es lässt sich sowohl die Art des Zugriffs (Lesen, Schreiben, Ausführen) festlegen, als auch der Zugriff auf bestimmte Geräte beschränken.

Grundsätzlich sollten Geräte nur sehr restriktiv zugelassen werden. Des Weiteren dürfen Anwender keine Programme aus Verzeichnissen starten können, auf die sie Schreibzugriff haben. Dies gilt auch für USB-Medien.

Die folgenden Einstellungen finden sich in den Gruppenrichtlinien unter folgendem Pfad: Start → Ausführen → Gpedit.msc → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Administrative Vorlagen → System → Wechselmedienzugriff

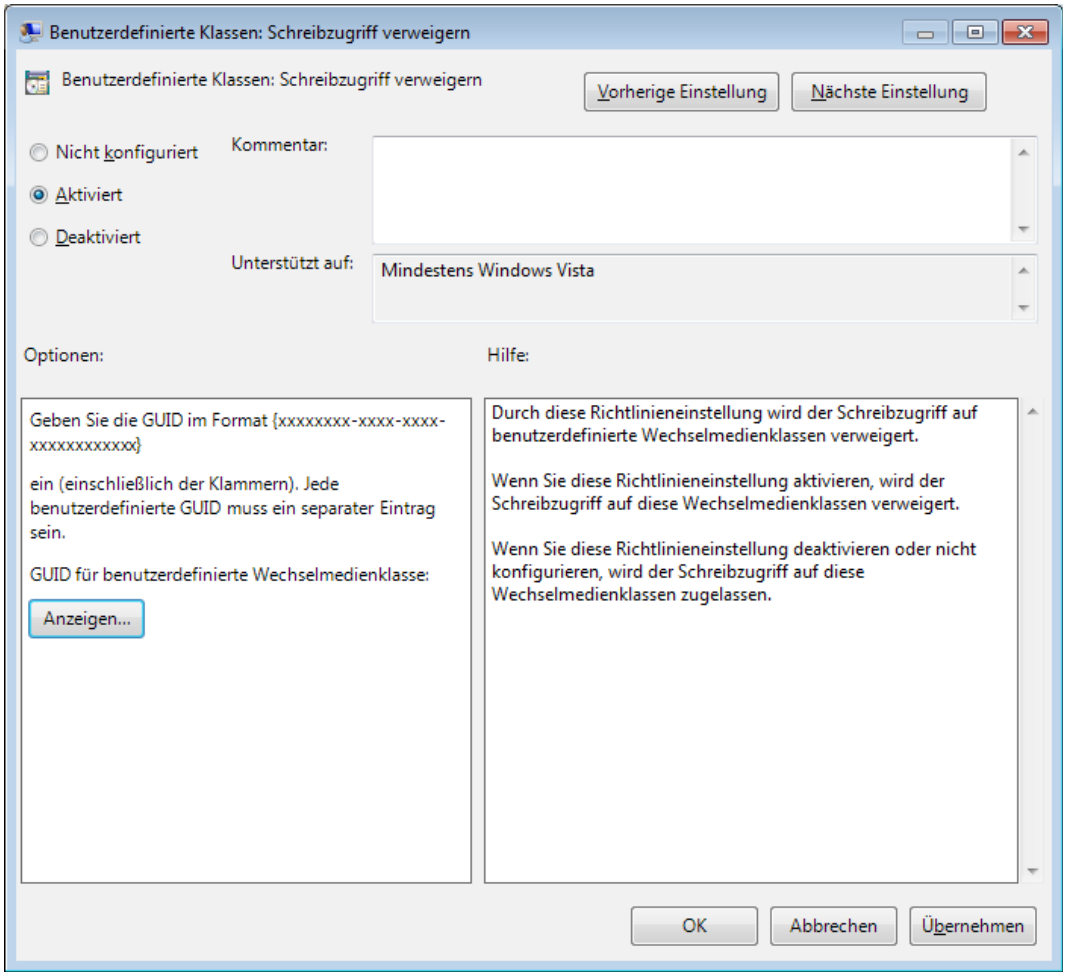


Abbildung 4.13: Konfiguration benutzerdefinierter Geräteklassen

CD und DVD: Ausführungszugriff verweigern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Disketten laufwerke: Ausführungszugriff verweigern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Wechseldatenträger: Ausführungszugriff verweigern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Bandlaufwerke: Ausführungszugriff verweigern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Zum Sperren des Lesezugriffs auf Benutzerdefinierte Geräte
Die Geräteklassen-GUID des jeweiligen Gerätes findet sich im Gerätemanager unter Eigenschaften des Gerätes → Details → Geräteklassen-GUID
Benuzerdefinierte Klassen: Lesezugriff verweigern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert und Eintrag der Geräte-GUID

Benuzerdefinierte Klassen: Schreibzugriff verweigern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert und Eintrag der Geräte-GUID

WPD-Geräte: Lesezugriff verweigern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

WPD-Geräte: Schreibzugriff verweigern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

4.2.9 Auslagerungsdatei

Die Auslagerungsdatei[85] (Swapfile) enthält Ausschnitte des physischen Speichers. Wenn die Kapazität des Arbeitsspeichers nicht mehr ausreicht, werden Teile des Speichers in diese Datei ausgelagert. Die Auslagerungsdatei sollte bei jedem Herunterfahren des APCs gelöscht werden, da sie sensible Informationen enthalten kann[86].

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computer-konfiguration → Windows-Einstellungen → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Herunterfahren: Auslagerungsdatei des virtuellen Arbeitsspeichers löschen

85 http://windows.microsoft.com/de-DE/windows7/What-is-virtual-memory
86 http://technet.microsoft.com/de-de/library/cc740219(WS.10).aspx

Default-Wert	Deaktiviert
Neuer Wert	Aktiviert

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFilesAtShutdown`

Default-Wert	0
Neuer Wert	1

4.2.10 LAN Manager Authentifizierungsebene

Die LAN Manager Authentifizierungseinstellungen[87] bestimmen die Authentifizierungsprotokolle für Netzwerkanmeldungen und die dafür eingesetzten Verfahren. Eine Fehleinstellung kann zu Kompatibilitätsproblemen mit anderen (älteren) IT-Systemen im Netzwerk führen[88].

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Windows-Einstellungen → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Netzwerksicherheit: LAN Manager-Authentifizierungsebene

Default-Wert	nicht konfiguriert
Neuer Wert	Nur NTLMv2-Antworten senden\LM & NTLM verweigern

`HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Control\Lsa\`
Neues REG_DWORD
Name: LmCompatibilityLevel

Default-Wert	Nicht vorhanden
Neuer Wert	5

4.2.11 Druckertreiber

APCs sollten nur die für ihren Arbeitsbereich zugewiesene Druckertreiber verwenden. Durch die Modifikation der Druckerkonfiguration besteht die Möglichkeit einer Kompromittierung des APCs. Daher sollten über die lokale Sicherheitsrichtlinie entsprechende Maßnahmen getroffen werden.[89]

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Windows-Einstellungen → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Geräte: Anwendern das Installieren von Druckertreibern nicht ermöglichen

Default-Wert	Deaktiviert
Neuer Wert	Aktiviert

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Drucker → Neue Drucker automatisch in Active-Directory veröffentlichen

Default-Wert	nicht konfiguriert
Neuer Wert	Deaktiviert

87 http://technet.microsoft.com/de-de/library/cc738867(WS.10).aspx
88 http://technet.microsoft.com/de-de/library/cc755344(WS.10).aspx
89 http://technet.microsoft.com/de-de/library/cc787926(WS.10).aspx

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Drucker → Installation von Druckern, die Kernelmodustreiber verwenden, nicht zulassen

Default-Wert	nicht konfiguriert
Neuer Wert	Aktiviert

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Drucker → Löschen von öffentlichen Druckern zulassen

Default-Wert	nicht konfiguriert
Neuer Wert	Aktiviert

Start → Ausführen → `Gpedit.msc` → Rechtsklick → „Als Administrator ausführen“ → Computerkonfiguration → Administrative Vorlagen → Drucker → Druckertreiberinstallations-Assistent – Netzwerksuchseite (Nicht verwaltetes Netzwerk)

Default-Wert	nicht konfiguriert
Neuer Wert	Deaktiviert

4.3 Absicherung der Betriebssystemdienste

Dieses Kapitel geht auf die Absicherung der Betriebssystemdienste (kurz: Dienste) ein. Abhängigkeiten, die zwischen Diensten bestehen können, werden in Abschnitt 4.3.1 erläutert. Danach wird in Abschnitt 4.3.2 die Vorgehensweise zur Konfiguration von Diensten beschrieben. Abschnitt 4.3.3 versucht eine Klassifizierung der Dienste in notwendig, optional und nicht-notwendig vorzunehmen. Dienste aus den Kategorien optional und nicht-notwendig werden dann in den Abschnitten 4.3.4 und 4.3.5 deaktiviert.

4.3.1 Abhängigkeiten zwischen Diensten

Benötigen Dienste und/oder Anwendungen für die Ausübung Ihrer Funktion explizit einen anderen Dienst und/oder eine andere Anwendung, so sind dies direkte Abhängigkeiten. Solche Abhängigkeiten lassen sich z. B. über die Diensteinstellung oder Herstellerangaben ermitteln (siehe Abbildung 4.15).

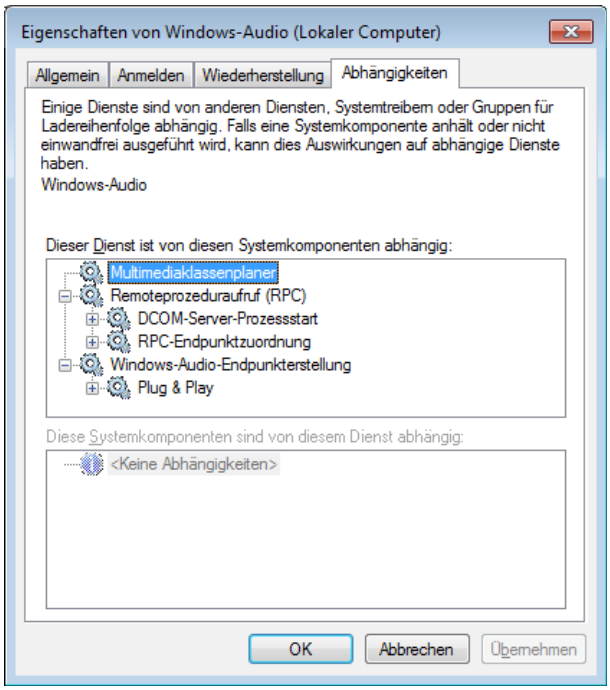


Abbildung 4.14: Abhängigkeiten in der GUI

Über die Registry kann ermittelt werden, welche Abhängigkeiten für den Start eines Dienstes zu anderen Diensten bestehen. Hierzu ist der Wert `DependOnService` im folgenden Schlüssel einzusehen:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\
[$SERVICE]\DependOnService
```

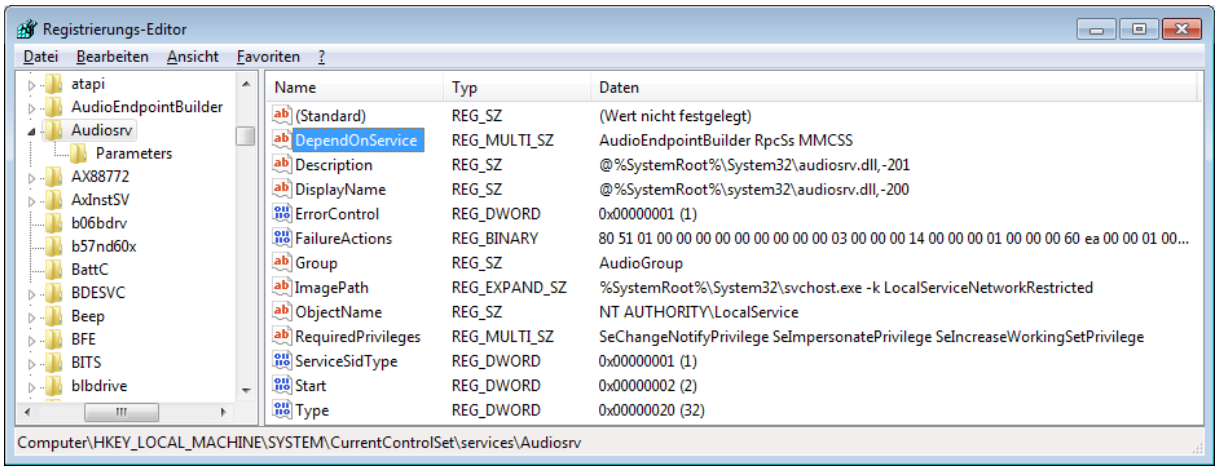


Abbildung 4.15: Abhängigkeiten in der Registry

Mit dem zusätzlichen Programm Dienstabhängigkeitsbetrachter (engl. Windows Service Dependency Viewer[90]) wird eine verbesserte Übersicht über die verschiedenen Dienste und Prozesse angeboten. Hier können auch die einzelnen Dienste den Prozessen zugeordnet werden.

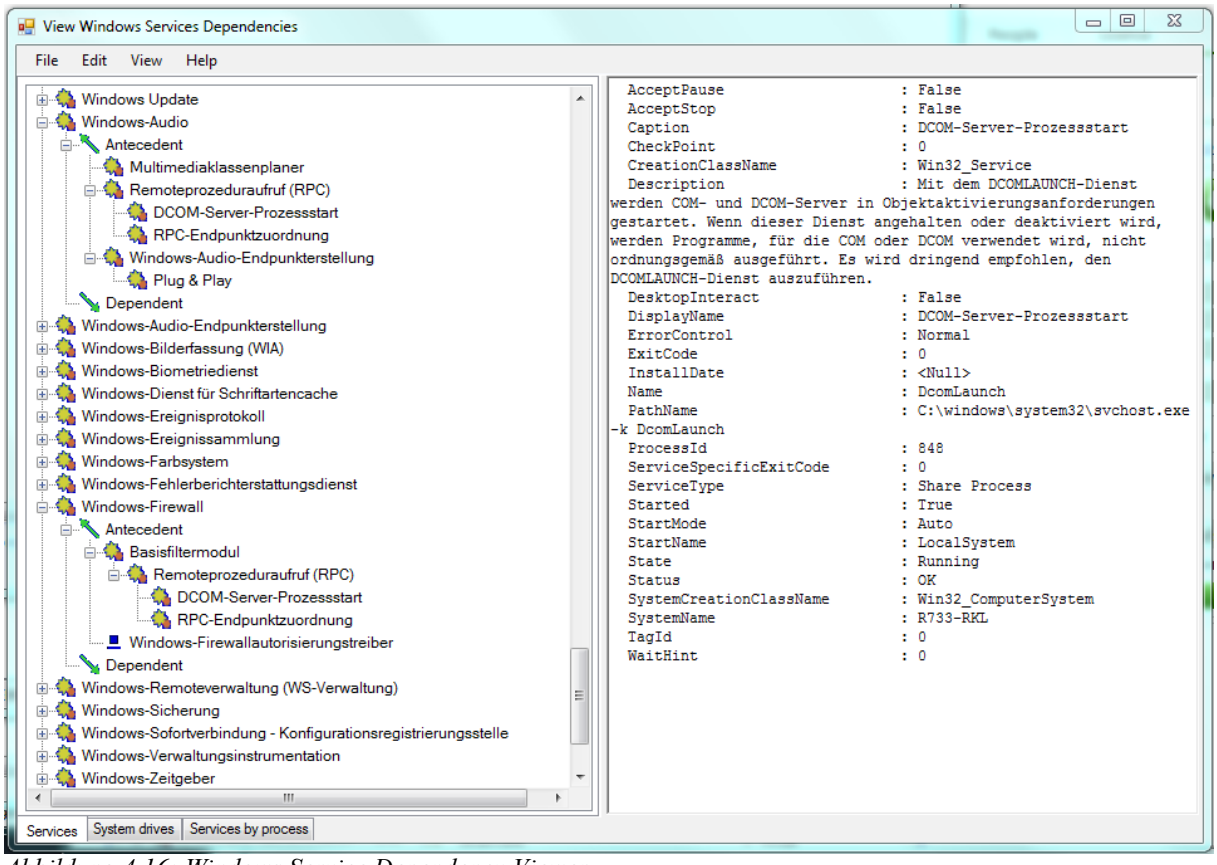


Abbildung 4.16: Windows Service Dependency Viewer

Tabelle 13 auf Seite 41 gibt einen Überblick über die Abhängigkeiten.

90 http://svcdependencyviewer.codeplex.com/

4.3.2 Vorgehensweise zur Deaktivierung von Diensten

Wie bereits in dem vorherigen Abschnitt beschrieben, werden auch in diesem Abschnitt die nachfolgenden drei Werkzeuge Registry, GUI und GPO mit den jeweils entsprechenden Symbolen verwendet.

4.3.2.1 Registry

Wird eine Härtung eines Dienstes über den Registrierungseditor vorgenommen, so wird immer der folgende Registrierungspfad verwendet:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\`

Die folgende Abbildung 4.17 zeigt beispielhaft die Einstellung des Dienstes Anwendungserfahrung über den Registrierungseditor:

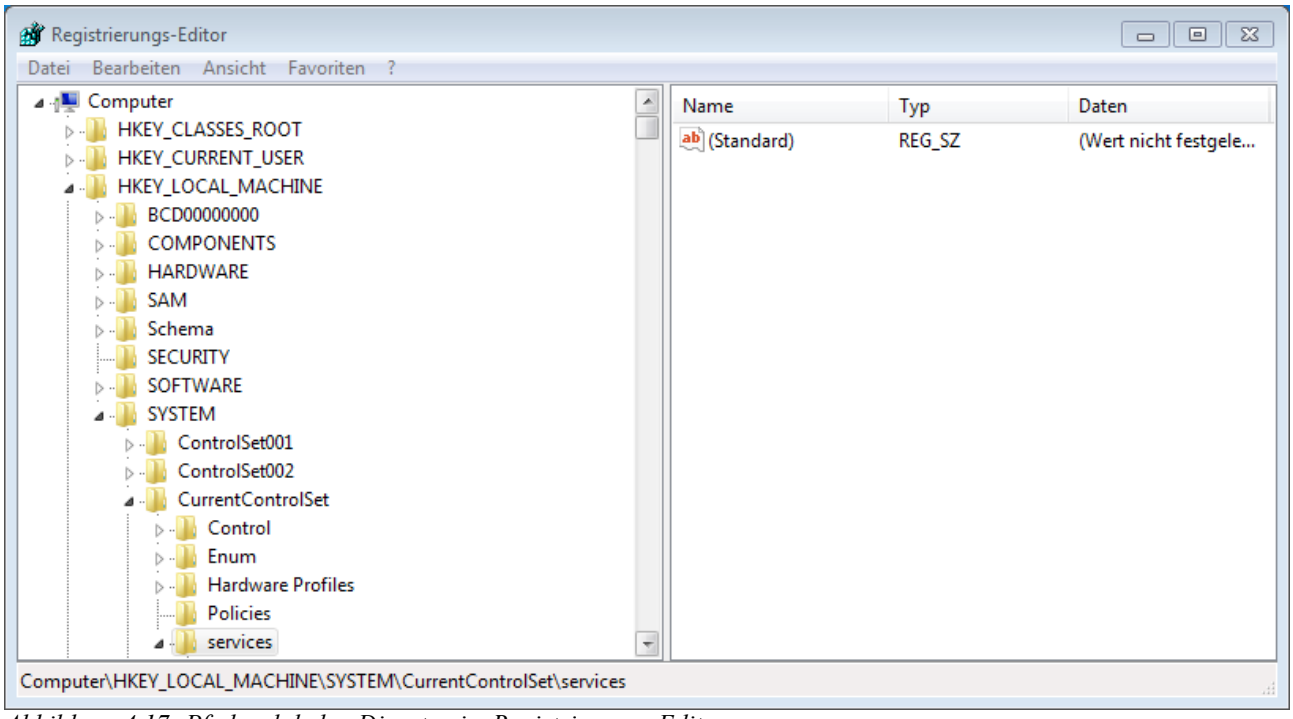


Abbildung 4.17: Pfad zu lokalen Diensten im Registrierungs-Editor

4.3.2.2 GUI

Wird eine Härtung der Dienste über die GUI vorgenommen, so wird immer die folgende Aktion ausgeführt

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Die folgende Abbildung 5.1 zeigt beispielhaft die Einstellung des Dienstes Adaptive Helligkeit:

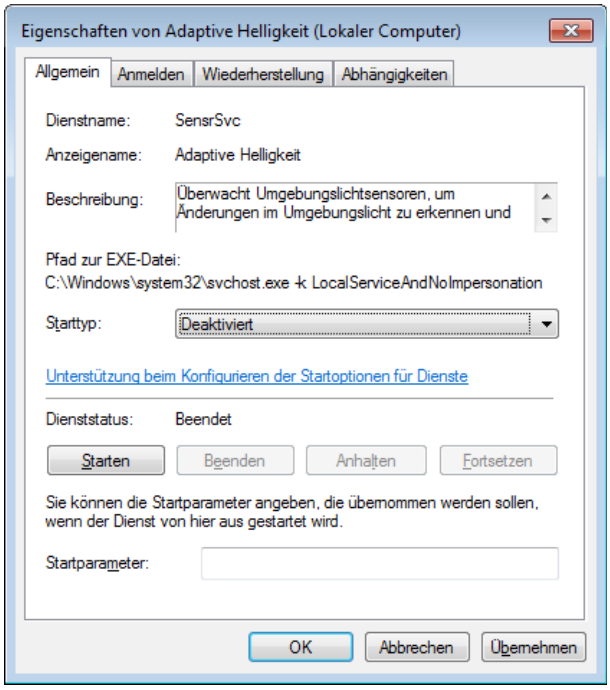


Abbildung 4.18: Eigenschaften eines Dienstes in der GUI

4.3.2.3 GPO

Bei Windows 7 werden die lokalen Dienste in der lokalen GPO (gpedit.msc) nicht aufgeführt. Daher werden in den nachfolgenden Abschnitten 4.3.4 und 4.3.5 zusätzlich die Möglichkeiten der GPO-Einstellungen mittels eines Windows 2008 R2 Domänenkontrollers aufgezeigt. Die Härtung wird über den Gruppenrichtlinienverwaltungs-Editor vorgenommen. Die GPOs für die jeweiligen Dienste finden Sie unter `<konstanter_Pfad><Dienst>`. In den folgenden Abschnitten 4.3.4 und 4.3.5 wird nur der Dienst-spezifische Teil der GPO detailliert angegeben. Der konstante Pfad wird als `<DC2008R2_GPO_HÄRTUNG>` angegeben und entspricht:

Start → Verwaltung → Gruppenrichtlinienverwaltung → Gruppenrichtlinienverwaltung → Gesamtstruktur → Domänen → [Auswahl der entsprechenden Domäne] → Gruppenrichtlinienobjekte → Rechtsklick → Neu → Eingabe des Namens (z. B. Services) → Ok → Rechtsklick auf das neue Gruppenrichtlinienobjekt (z. B. Services) → Bearbeiten → Der Gruppenrichtlinienverwaltungs-Editor öffnet sich → Computerkonfiguration → Richtlinien → Windows-Einstellungen → Sicherheitseinstellungen → Systemdienste → Rechtsklick auf den Dienstname → Eigenschaften → Haken bei „Diese Richtlinieneinstellung definieren“ setzen. Schalter bei „Deaktiviert“ setzen. → Übernehmen → Schließen des der Gruppenrichtlinienverwaltungs-Editors → Zurück zum Fenster der Gruppenrichtlinienverwaltung gehen → Rechtsklick auf die entsprechende Organisationseinheit der Windows 7 APCs → Vorhandenes Gruppenrichtlinienobjekt verknüpfen... → Auswahl der neuen Gruppenrichtlinie (z. B. Services) → Wechsel zum APC → Start → Alle Programme → Zubehör → Eingabeaufforderung → Eingabe von gpupdate /force

Achtung: Der Domänenkontroller muss zur Bereitstellung eines Active-Directory entsprechend vorkonfiguriert sein[91]. Ebenfalls ist sicher zu stellen, dass sich die zu härtenden Windows 7 APCs in einer entsprechende Organisationseinheit[92] des AD befinden, damit die GPO-Richtlinien nicht auch auf anderen Rechnern dieser Domäne (z. B. auf den Domänenkontroller selbst) angewendet werden.

91 http://technet.microsoft.com/de-de/library/cc755258(WS.10).aspx
92 http://technet.microsoft.com/en-us/library/cc753063.aspx

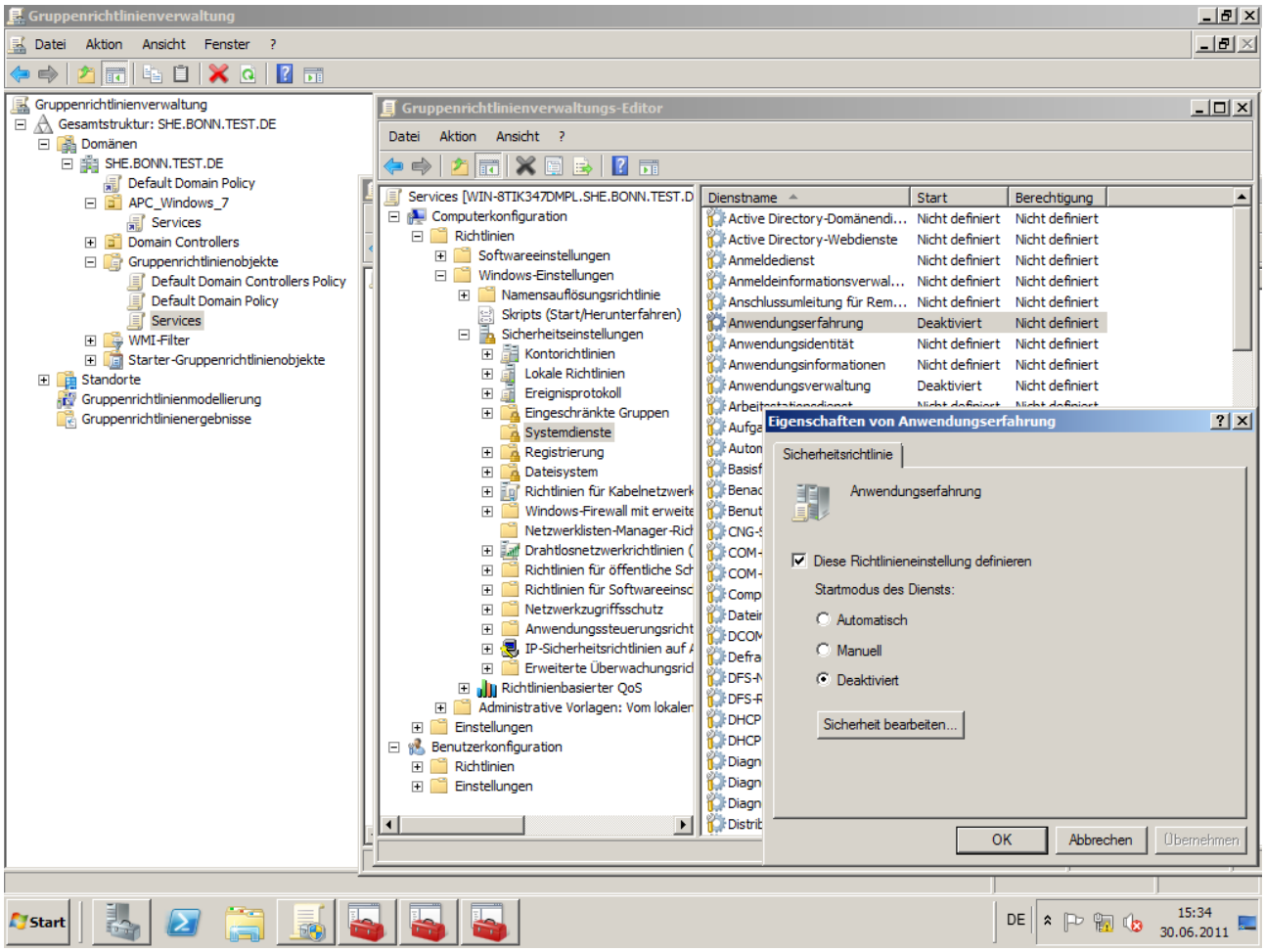


Abbildung 4.19: Gruppenrichtlinienverwaltungs-Editor unter Windows 2008 R2

4.3.3 Notwendigkeit der Dienste

Im Rahmen der Minimierung sind nicht benötigte Dienste des APCs zu deaktivieren. Die Deaktivierung von Diensten schränkt die Funktionalität ein, was Auswirkungen auf Komponenten, Anwendungen und die Benutzerfreundlichkeit haben kann, wie beispielsweise:

- Der Start/Installation einer nicht in diesem Dokument spezifizierten Anwendung schlägt fehl.
- Die Kommunikation über bestimmte Protokolle (z. B. PNRP) ist nicht möglich.
- Das Durchschleifen von Druckern und Laufwerken über Terminalverbindungen ist nicht mehr möglich.

Um die im Abschnitt 2.5 betrachteten zusätzlichen Anwendungen ohne funktionale Einschränkungen verwenden zu können, sind die Dienste in notwendige, optionale und nicht-notwendige Dienste zu unterteilen. Es ist vom Systemverantwortlichen zu prüfen, ob der zu härtende Dienst in der Organisation in Verwendung ist, oder ob dieser deaktiviert werden kann. Grundsätzlich können alle als optional definierten Dienste (siehe Abschnitt 4.3.4) deaktiviert werden. Die Deaktivierung hat keine negativen Auswirkungen auf die in diesem Dokument definierten Anforderungen.

Notwendige Dienste:	Dieser Dienst wird zur einwandfreien Funktion von Windows 7 und/ oder den zusätzlichen Anwendungen benötigt und sollte nicht deaktiviert werden.
Optionale Dienste:	Dieser Dienst kann Einfluss auf die Funktion der zusätzlichen Anwendungen oder Windows 7 direkt haben. Es ist zu prüfen, ob der Dienst in der Organisation in Verwendung ist, oder ob dieser deaktiviert werden kann.
Nicht notwendige Dienste:	Dieser Dienst wird weder von der Windows 7 Betriebssystem Basis, noch von zusätzlichen Anwendungen benötigt und kann daher deaktiviert werden. Die Starteinstellungen sollten entsprechend den Angaben in Abschnitt 4.3.5 verändert werden. Liegt ein zwingend notwendiger Grund zur Verwendung dieses Dienstes vor, so ist eine Sicherheitsbetrachtung durchzuführen.

Tabelle 15 stellt die Einteilung der Dienste vor.

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
ActiveX-Installer (AxInstSV)		X		Wird für ActiveX-Steuerelemente benötigt. Bei einer Deaktivierung werden ActiveX-Steuerelemente anhand der Einstellungen des Standardbrowser eingestellt.
Adaptive Helligkeit			X	Passt die Bildschirmhelligkeit der Umgebung an. Wird nur bei einem mobilen APC benötigt.
Anmeldedienst	X			Unterstützt einen sicheren Kanal zwischen APC und Domänen-Controller zum Authentifizieren von Benutzern und Diensten.
Anmeldeinformationsverwaltung		X		Wird für das Abrufen von Anmeldeinformationen benötigt (z. B. gespeicherte Biometriedaten). Dieser Dienst kann deaktiviert werden, wenn die zusätzlichen Sicherheitsfunktion nicht benötigt werden.
Anschlussumleitung für Remotedesktopdienst im Benutzermodus			X	Leitet Drucker und Laufwerke in Terminalverbindungen (RDP) um. Es sollten geeignetere Technologien für den Zugriff auf Laufwerke und Drucker verwendet werden.
Anwendungserfahrung		X		Wird nur benötigt, wenn die AERO-Benutzeroberfläche und der Windows-XP Kompatibilitätsmodus in Verwendung ist.
Anwendungsidentität	X			Bestimmt und überprüft die Identität einer Anwendung. (Starttyp manuell)
Anwendungsinformationen	X			Ermöglicht das Starten von Programmen mit erweiterten Privilegien mittels der Benutzerkontensteuerung (Starttyp manuell).
Anwendungsverwaltung	X			Wird für das Installieren und Deinstallieren von mittels Gruppenrichtlinien verwalteten Programmen benötigt.
Arbeitsstationsdienst	X			Wird für Zugriffe auf Netzwerkfreigaben und andere Ressourcen (z.B. Drucker) benötigt.
Aufgabenplanung	X			Dieser Dienst arbeitet automatisch die geplanten Aufgaben ab (z.B. Updates, Zeitsynchronität).
Automatische Konfiguration (verkabelt)		X		Ist für die Authentifikation über 802.1x zuständig. Wird 802.1x im Netzwerk nicht verwendet, kann dieser Dienst deaktiviert werden.
Automatische WLAN-Konfiguration		X		Ist für die Verwaltung von WLAN-Karten und -Profilen zuständig. Wird im Netzwerk kein WLAN verwendet, kann dieser Dienst abgeschaltet werden.
Basisfiltermodul	X			Das Basisfiltermodul ist ein Dienst, der Firewall- und IPsec-Richtlinien überwacht und eine Benutzermodusfilterung implementiert. Der Dienst Windows Firewall ist von diesem Dienst abhängig.
Benachrichtigungsdienst für Systemereignisse			X	Teilt dem Anwender Informationen über den Zustand des APC mit. Mobile Arbeitsstationen benutzen diesen Dienst für entsprechende Aktivitäten bei niedrigem Batteriestatus! Daher sollte bei dieser Geräteklasse dieser Dienst nicht deaktiviert werden.

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
Benutzerprofildienst	X			Wird für die lokale Anmeldung benötigt und darf nicht deaktiviert werden.
BitLocker-Laufwerkverschlüsselungsdienst		X		Ermöglicht einen gesicherten Systemstart und Laufwerksverschlüsselungen. Wird der Dienst deaktiviert, können die lokalen Laufwerke nicht mehr ver-/entschlüsselt werden.
Blockebenen-Sicherungsmodul		X		Wird für die Wiederherstellung und Sicherung des Betriebssystems verwendet. Notwendig für eine lokale Wiederherstellung des Systems. Daher sollte der Dienst nur bei der Verwendung einer zusätzlichen Wiederherstellungssoftware deaktiviert werden.
Bluetooth-Unterstützungsdienst		X		Ermöglicht die Erkennung und Verwaltung von Bluetooth-Geräten (z. B. Kopfhörer).
BranchCache		X		Dieser Dienst speichert Netzwerkinhalte des lokalen Subnetzes und kann die Geschwindigkeit von Datenzugriffen erhöhen.
CNG-Schlüsselisolation	X			Ist für die sichere Speicherung von privaten Schlüsseln zuständig.
COM+-Ereignissystem	X			Unterstützt den Systemereignis-Benachrichtigungsdienst (SENS), mit dem Ereignisse automatisch an abonnierende COM-Komponenten verteilt werden.
COM+-Systemanwendung	X			Verwaltet und überwacht COM-Komponenten.
Computerbrowser			X	Ermittelt alle Computer und Freigaben in einem Netzwerk und teilt diese Informationen auch anderen Systemen mit. Der Dienst wird nicht zwingend benötigt und kann deaktiviert werden.
DCOM-Server-Prozessstart	X			Wird vom RPC benötigt und darf nicht beendet werden, da er für die DCOM-Dienste die Startfunktionalität bietet.
Defragmentierung		X		Bietet die Funktion zur Defragmentierung von Laufwerken und die Möglichkeit zur Leistungssteigerung. Wird die Defragmentierung für die Laufwerke nicht benötigt, kann dieser Dienst deaktiviert werden.
Designs		X		Wird für die AERO-Desktopoberfläche benötigt. Wird nur mit der „klassischen Oberfläche“ gearbeitet, kann dieser Dienst deaktiviert werden.
DHCP-Client	X			Registriert und aktualisiert IP-Adressen und DNS-Einträge für diesen Computer. Der APC kann keine dynamischen IP-Adressen und DNS-Aktualisierungen über DHCP empfangen, falls dieser Dienst beendet wird.
Diagnosediensthost			X	Ermöglicht Diagnosen im Kontext lokaler Dienste.
Diagnoserichtliniendienst			X	Dieser Dienst ermöglicht die Erkennung, Behandlung und Lösung von Problemen für Windows-Komponenten.
Diagnosesystemhost			X	Ermöglicht Diagnosen im lokalen System-Kontext.

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
Distributed Transaction Coordinator		X		Koordiniert Transaktionen, die sich über mindestens zwei Ressourcenverwaltungen wie Datenbanken, Nachrichtenwarteschlangen oder Dateisysteme erstrecken.
DNS-Client	X			Der DNS-Clientdienst speichert DNS-Namen (Domain Name System) zwischen und registriert den vollständigen Computernamen für diesen Computer.
Druckwarteschlange	X			Wird benötigt, wenn auf diesem Rechner ein Drucker installiert werden soll oder Daten an einen Drucker gesendet werden müssen. Dieser Dienst sollte nur dann deaktiviert werden, wenn mit dem APC nicht gedruckt werden muss.
Enumeratordienst für tragbare Geräte	X			Dieser Dienst überträgt Gruppenrichtlinien auf Wechsel-Massenspeicher-Geräte, wie DVD-Rom.
Erkennung interaktiver Dienste		X		Ermöglicht Kommunikation zwischen Diensten und der Benutzeroberfläche über Dialogfelder.
Extensible Authentication Protokoll	X			Wird dieser Dienst beendet, können Clients mittels EAP (z. B. 802.1x, VPN, NAP) nicht mehr kommunizieren.
Fax			X	Ermöglicht das Senden und Empfangen von Faxen mithilfe der Fax-Ressourcen. Dieser Dienst kann deaktiviert werden.
Funktionssuchanbieter-Host			X	Dieser Dienst stellt Basisfunktionen bereit, die von anderen Diensten zur Diensteerkennung und Plug&Play (z.B. SSDP, WS-D) im Netzwerk genutzt werden. Dieser Dienst kann deaktiviert werden.
Funktionssuche-Ressourcenveröffentlichung			X	Informationen über angeschlossene Geräte werden im lokalen Netz weitergeleitet.
Gatewaydienst auf Anwendungsebene			X	Dieser Dienst stellt Funktionen für die gemeinsame Nutzung von Internetverbindungen bereit und sollte auf einem lokalen APC deaktiviert werden.
Gemeinsame Nutzung der Internetverbindung			X	Bietet für lokale APCs die Möglichkeit, über diesen Dienst/APC gemeinsam auf Ressourcen im Internet zuzugreifen. Dieser Dienst sollte auf einem lokalen APC deaktiviert werden.
Geschützter Speicher	X			Passwörter und Schlüssel werden in einem geschützten Speicher abgelegt.
Gruppenrichtlinienclient	X			Dieser Dienst wird für die Verwaltung des APCs mittels Gruppenrichtlinien benötigt.
Heimnetzgruppen-Anbieter			X	Dieser Dienst ist nur für die Konfiguration von Computern erforderlich, die einer Heimnetzgruppe zugeordnet sind, und kann beim Betrieb in einer Domäne deaktiviert werden.
Heimnetzgruppen-Listener			X	Dieser Dienst ist nur für die Konfiguration von Computern erforderlich, die einer Heimnetzgruppe zugeordnet sind, und kann beim Betrieb in einer Domäne deaktiviert werden.
IKE- und AuthIP IPSec-		X		Dieser Dienst wird für die Verwendung von IPSec

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
Schlüsselerstellungsmodule				benötigt. Wird mit dem APC keine IPSec-Verbindung aufgebaut, kann der Dienst deaktiviert werden. Achtung: Einige Softwarehersteller verwenden diesen Dienst für Ihre IPSec-Clients.
Integritätsschlüssel- und Zertifikatverwaltung	X			Wird für die Benutzung von X.509 Zertifikaten verwendet (z. B. HTTPS, S/MIME, EFS).
Intelligenter Hintergrundübertragungsdienst	X			Integrierter Downloadmanager, der verzögert startet.
IP-Hilfsdienst			X	Ermöglicht IPv6-Verbindungen über IPv4-Netze und wird nur benötigt, wenn Ipv6-Tunneltechniken verwendet werden sollen. Daher kann dieser Dienst deaktiviert werden.
IPSec-Richtlinien-Agent	X			Sichert und kontrolliert in Windows die Übertragung von IP-Paketen.
Konfiguration für Remotedesktops		X		Der Dienst ist für alle Konfigurations- und Sitzungsverwaltungsaktivitäten im Zusammenhang mit den Remotedesktopdiensten und Remotedesktop zuständig. Wird RDP nicht benötigt, kann dieser Dienst deaktiviert werden.
Kryptografiedienste	X			Dieser Dienst ist für die Bestätigung von Signaturen und das Hinzufügen von Zertifikaten erforderlich. Diese Mechanismen werden auch bei der Installation von Anwendungen und beim Windows-Update verwendet.
KtmRm für Distributed Transaction Coordinator			X	Ist eine Stabilitäts- und Sicherheitsfunktion für den Dienst „Distributed Transaction Coordinator“.
Leistungsindikator-DLL-Host			X	Ermöglicht Informationsabfragen von 32-Bit DLL Dateien zur Ermittlung von Leistungsdaten.
Leistungsprotokolle und -warnungen			X	Leistungsinformationen werden erfasst und entsprechende Warnungen in ein Logverzeichniss geschrieben.
Media Center Extender-Dienst			X	Ermöglicht externen Geräten (z. B. XBOX) das Suchen des Computers und den Verbindungsaufbau.
Microsoft .NET Framework NGEN v2.0.50727_X64	X			Wird für Systemupdates benötigt.
Microsoft iSCSI-Initiator-Dienst			X	Der Dienst ermöglicht die Verbindung mit iSCSI-Geräten im Netzwerk. iSCSI wird vermehrt im Server- und Speicherbereich angewendet und kann daher auf einem APC deaktiviert werden.
Microsoft-Softwareschatten-kopie-Anbieter		X		Verwaltet die vom Dienst „Volumenschattenkopie“ erstellten Abbilder. Er ist notwendig, wenn der oben genannte Dienst verwendet wird.
Multimediaklassenplaner	X			Wird von dem Dienst „Windows-Audio“ benötigt und darf nicht abgeschaltet werden.
NAP-Agent (Network Access Protection)	X			Dieser Dienst sammelt Informationen über den APC, die dann beim Eintritt in eine Domäne mit den vorgegebenen Sicherheitsrichtlinien abgeglichen werden.

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
Net.Tcp-Portfreigabedienst			X	Ermöglicht es TCP-Ports mit anderen Rechnern im Netzwerk zu teilen.
Netzwerklistendienst	X			Identifiziert die Netzwerke, mit denen der Computer eine Verbindung hergestellt hat, sammelt und speichert Eigenschaften für diese Netzwerke, und benachrichtigt Anwendungen, wenn sich diese Eigenschaften ändern.
Netzwerkspeicher-Schnittstellendienst	X			Dieser Dienst ist für Netzwerkverbindungen erforderlich.
Netzwerkverbindungen	X			Verwaltet Objekte im Ordner "Netzwerk- und Wählverbindungen", in dem LAN- Remoteverbindungen angezeigt werden.
NLA (Network Location Awareness)	X			Dieser Dienst sammelt und speichert Konfigurationsinformationen für das Netzwerk und benachrichtigt Programme, wenn diese Informationen geändert werden.
Offlinedateien		X		Gleicht Offline-Daten beim Anmeldevorgang zwischen lokalem Zwischenspeicher und Remotespeicherplatz ab. Diese Funktionalität kann deaktiviert werden, wenn nicht mit Dateien in einem Netzwerk gearbeitet wird.
Parental Controls			X	Dieser Dienst ist für die Abwärtskompatibilität der Jugendschutzfunktion vorhanden und kann deaktiviert werden.
Peer Name Resolution-Protokoll			X	Wird für Peer-to-Peer Netzwerke benötigt, wenn eine Namensauflösung ohne DNS möglich sein soll. Der Dienst kann deaktiviert werden. Windows-Teamarbeit oder Windows-Besprechungen benötigen allerdings diesen Dienst.
Peernetzwerk-Gruppenzuordnung			X	Ordnet die Peer-to-Peer Netze Gruppen zu und wird z. B. für Windows-Teamarbeit oder Windows-Besprechungen benötigt. Dieser Dienst kann deaktiviert werden.
Peernetzwerkidentitäts-Manager			X	Identifiziert die Peer-to-Peer Netze und wird z. B. für Windows-Teamarbeit oder Windows-Besprechungen benötigt. Dieser Dienst kann deaktiviert werden.
Plug & Play	X			Ermöglicht dem Computer, Hardware zu erkennen und sich ohne oder mit geringer Benutzerinteraktion darauf einzustellen.
PnP-X-IP-Busenumerator			X	Erkennt automatisch PnP-Geräte im Netzwerk und wird z. B. für Windows-Media-Center benötigt.
PNRP-Computernamenveröffentlichungs-Dienst			X	Ermöglicht dynamische Namensveröffentlichungen über Peer-to-Peer Netzwerke und wird hauptsächlich für IPv6 verwendet.
Programmkompatibilitäts-Assistent-Dienst			X	Verbessert die Kompatibilität von Anwendungen mit dem Betriebssystem.
RAS-Verbindungsverwaltung			X	Wird nur benötigt, wenn über ein Modem VPN-

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
				oder ISDN-Verbindungen hergestellt werden müssen. Dieser Dienst kann deaktiviert werden.
Remotedesktopdienste		X		Wird benötigt, wenn der Rechner beispielsweise remote administriert werden soll.
Remoteprozeduraufruf (RPC)	X			Der RPCSS-Dienst wird als Dienst-steuerungs-Manager für COM2- und DCOM-Server verwendet. Von ihm werden Objektaktivierungs-anforderungen, Objektexporterauflösungen und die verteilte Garbage Collection für COM2- und DCOM-Server ausgeführt. Von diesem Dienst sind weitere 69 Dienste abhängig.
Remoteregistrierung			X	Dieser Dienst ermöglicht Administratoren den Fernzugriff auf die lokale Registrierungsdatei.
Richtlinie zum Entfernen der Smartcard		X		Regelt die Aktion bei Entfernen einer Smartcard (z. B. Sperren des Bildschirms). Der Dienst kann dann deaktiviert werden, wenn keine Aktionen beim Entfernen der Smartcard geplant sind oder keine Smartcard in Verwendung ist.
Routing und RAS			X	Ermöglicht zwischen einem Netzwerkverbund die Möglichkeit der Paketweiterleitung (engl. Routing). Bei einem APC wird diese Funktion nicht verwendet und kann deaktiviert werden.
RPC-Endpunktzuordnung	X			Dieser Dienst dient der Zuordnung von RPC-Schnittstellen und wird vom Betriebssystem benötigt.
RPC-Locator		X		Ist für die Verwaltung der RPC-Dienstnamendatenbank für verteilte Anwendungen im Netz zuständig.
Sekundäre Anmeldung		X		Wird für den automatischen Start von Anwendungen mit anderen Benutzerrechten benötigt (Funktion wie „Ausführen als“).
Server			X	Ermöglicht die Freigabe von Datei- und Druckerfreigaben für Dritte. Da diese Freigaben nicht benötigt werden, wird dieser Dienst deaktiviert.
Server für Threadsortierung	X			Optimiert die Reihenfolge für die Ausführungen von Threads im Kernel.
Shellhardwareerkennung			X	Erkennt eingelegte Medien und bietet die Auto-Play-Funktion an. Dieser Dienst wird nicht benötigt und kann deaktiviert werden. Beim Einlegen eines Mediums muss dann der entsprechende Vorgang manuell gestartet werden.
Sicherheitscenter	X			Der WSCSVC-Dienst (Windows-Sicherheitscenter) überwacht und meldet die Sicherheitsintegritätseinstellungen auf dem Computer. Zu diesen Einstellungen zählen Firewall (Ein/Aus), Virenschutzsoftware (Ein/Aus/nicht mehr aktuell), Antispyware (Ein/Aus/nicht mehr aktuell), Windows Update (Updates automatisch/manuell herunterladen und

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
				installieren), Benutzerkontensteuerung (Ein/Aus) und Interneteinstellungen (empfohlen/nicht empfohlen). Der Dienst wird vom Wartungscenter verwendet, um in der Benutzeroberfläche Systray-Warnungen und eine grafische Ansicht der Sicherheitsintegritätsstatus bereitzustellen.
Sicherheitskonto-Manager	X			Dieser Dienst signalisiert anderen Diensten, dass die Sicherheitskontenverwaltung (SAM) aktiv ist und speichert Sicherheitsinformationen lokaler Benutzerkonten.
Sitzungs-Manager für Desktop-fenster-Manager		X		Ist für Effekte (z. B. Transparenz, Mouseover) der AERO-Oberfläche verantwortlich und kann deaktiviert werden, wenn diese nicht benötigt werden.
Smartcard		X		Wird benötigt, um einen Zugriff auf Smartcards oder biometrische Leseeinheiten (z. B. Fingerabdruckleser) zu erhalten. Werden solche Funktionen nicht verwendet, sollte der Dienst deaktiviert werden.
SNMP-Trap		X		Dieser Dienst ermöglicht das Empfangen von SNMP-Trap-Nachrichten und das Weiterleiten an SNMP-Management-Stationen.
Software Protection	X			Aktiviert das Herunterladen, die Installation und die Durchsetzung digitaler Lizenzen für Windows und Windows-Anwendungen. Überprüft die Rechtmäßigkeit von Windows-Anwendungen und des Windows-Betriebssystem (z. B. Echtheit).
Speicherdienst	X			Der Speicherdienst wird für die Übermittlung der Einstellungen von Speichereigeräten mittels Gruppenrichtlinien benötigt.
SPP-Benachrichtigungsdienst	X			Dieser Dienst wird für die Aktivierung und Verwaltung von Softwarelizenzen benötigt.
SSDP-Suche			X	Bietet die Funktionalität zur Erkennung von UPnP-Geräten (z. B. Mediaplayer, XBOX) über das Netzwerk. Dieser Dienst kann deaktiviert werden.
SSTP-Dienst		X		Stellt eine sichere VPN-Verbindung zwischen einem APCs und einem Remotecomputer her. Dieser Dienst kann deaktiviert werden wenn sich die Rechner in der gleichen Schutzzone befinden.
Stromversorgung	X			Verwaltet die Energierichtlinien des APCs und wird dringend für den Dienst „Windows-Audio-Endpunkterstellung“ benötigt.
Superfetch		X		Beschleunigt den APC, da Anwendungen in entsprechende Bereiche der Festplatte geladen werden und benötigte Programme vor dem eigentlichen Gebrauch geladen werden.
Tablet PC-Eingabedienst			X	Ermöglicht die Eingabe mittels Finger oder Stift auf einer berührungssensitiven Oberfläche. Bei einem lokal aufgestellten APC kann dieser Dienst deaktiviert werden. Diese Komponente wurde bereits im Abschnitt 4.1 entfernt.

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
TCP/IP-NetBIOS-Hilfsdienst	X			Bietet Unterstützung für den NetBIOS-über-TCP/IP-Dienst (NetBT) und die NetBIOS-Namensauflösung für APCs im Netzwerk, so dass Benutzer Daten gemeinsam nutzen, drucken und sich am Netzwerk anmelden können. Diese Funktionen sind nicht mehr verfügbar, sofern dieser Dienst beendet wird.
Telefonie			X	Wird für Modem- oder Fax-Verbindungen benötigt und kann daher deaktiviert werden.
TPM-Basisdienste		X		Der TPM-Dienst ermöglicht den Zugriff auf Funktionen des TPM. Er kann deaktiviert werden, wenn kein TPM verwendet wird.
Überwachung verteilter Verknüpfungen (Client)			X	Verwaltet NTFS-Verknüpfungen auf und zwischen Computern und ändert diese, wenn diese z. B. verschoben werden.
Unterstützung in der Systemsteuerung unter Lösungen für Probleme			X	Der Dienst versendet Daten über Probleme auf dem System an Microsoft. Der Dienst kann deaktiviert werden.
UPnP-Gerätehost			X	Dieser Dienst stellt lokale UPnP-Geräte im Netzwerk zur Verfügung. Dieser Dienst kann deaktiviert werden.
Verbessertes Windows-Audio/Video-Streaming		X		Dieser Dienst stellt Netwerk-Quality of Service für Streaming sicher und kann i.d.R. deaktiviert werden. Wird das Streaming für Anwendungen wie dem Media Player verwendet, sollten die Standardeinstellungen verwendet werden.
Verbindungsschicht-Topologieerkennungs-Zuordnungsprogramm			X	Ermittelt die Ressourcen der Netzwerkschicht und zeigt den Status der verbundenen Geräte an. Dieser Dienst kann deaktiviert werden.
Verschlüsselndes Dateisystem (EFS)		X		Der Dienst ermöglicht die Verschlüsselung von Dateien oder Ordnern mittels EFS. Wird die Funktion nicht verwendet, kann der Dienst deaktiviert werden.
Verwaltung für automatische RAS-Verbindung			X	Stellt Verbindungen über Dial-UP oder DSL her. Dieser Dienst wird auf einem APC nicht benötigt.
Virtueller Datenträger			X	Verwaltet unterschiedliche Datenträger und fasst diese zusammen, ohne dass durch den jeweiligen Hersteller eine eigene Verwaltungsapplikation bereitgestellt werden muss. Der Dienst kann für einen APC deaktiviert werden.
Volumeschattenkopie			X	Der Dienst ermöglicht die Erstellung von Schattenkopien. Dabei werden neue Daten erstellt, die alten jedoch nicht überschrieben. Dieser Dienst kann beim APC deaktiviert werden.
WebClient			X	Ermöglicht Anwendungen wie Frontpage Internet-Dateien zu erstellen und mittels WebDav zugänglich zu machen. Dieser Dienst kann auf dem APC deaktiviert werden.
Windows CardSpace			X	Verwaltet die digitalen Identitäten der Microsoft-eigenen Authentifizierung im Web.

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
Windows Defender		X		Der Dienst stellt Viren- und Spywareschutz zur Verfügung und sollte nur deaktiviert werden, wenn ein anderes Produkt installiert ist.
Windows Driver Foundation - Benutzermodus-Treiberframework	X			Ermöglicht die Installation und Nutzung von Benutzermodustreibern (UMDF).
Windows Installer	X			Über diesen Dienst werden Anwendungen installiert, deinstalliert oder repariert.
Windows Media Center-Empfängerdienst			X	Zeichnet TV-oder Radiosendungen auf, welche dann mit dem Windows Media Center wiedergegeben werden können. Diese Komponente wurde bereits im Abschnitt 4.1.2 entfernt.
Windows Media Center-Planer-dienst			X	Steuert den Start und das Ende von Aufnahmen welche über das Windows Media Center definiert werden. Diese Komponente wurde bereits im Abschnitt 4.1.2 entfernt.
Windows Media Player-Netzwerkfreigabedienst			X	Mittels UPnP werden digitale Medien an andere APCs im Netzwerk freigegeben.
Windows Modules Installer	X			Ermöglicht das Installieren, Ändern und Entfernen von Windows-Updates und optionalen Komponenten.
Windows Presentation Foundation-Schriftartcache 3.0.0.0		X		Dieser Dienst optimiert WPF-Anwendungen, indem er Schriftarten zwischenspeichert.
Windows Search	X			Wird für die Windows-interne Suchfunktion sowie die Indexierung verwendet.
Windows Update	X			Erkennung, Herunterladen und Installation von Updates für Windows und andere Programme. Wenn der Dienst deaktiviert ist, können "Windows Update" bzw. die Funktion "automatische Updates" nicht verwendet werden.
Windows-Audio	X			Dieser Dienst wird dringend für Audiofunktionen einer Standardsoftware (z. B. Windows-Media-Player) verwendet.
Windows-Audio-Endpunkterstellung	X			Dieser Dienst unterstützt „Windows-Audio“ bei der Verwaltung von Audiogeräten (z. B. Mikrofone, Lautsprecher) und darf nicht deaktiviert werden, wenn Audio gewünscht ist.
Windows-Bilderfassung (WIA)		X		Stellt die Schnittstelle zu Scannern und Kameras dar und sollte dann deaktiviert werden, wenn keine Bildbearbeitung gewünscht ist oder eine entsprechende Funktionalität eines Hersteller installiert wurde.
Windows-Biometriedienst			X	Hiermit werden biometrische Daten von Anwendungen erfasst, verglichen, verändert oder gespeichert. Der Dienst kann beim APC deaktiviert werden.
Windows-Dienst für		X		Ermöglicht das Zwischenspeichern von Schriften.

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
Schriftartencache				Eine Deaktivierung verlangsamt Anwendungen, welche auf unterschiedliche Schriftarten zugreifen.
Windows-Ereignisprotokoll	X			Dieser Dienst verwaltet Ereignisse und Ereignisprotokolle. Er unterstützt die Protokollierung, Abfrage und Abonnierung von Ereignissen sowie die Archivierung von Ereignisprotokollen und die Verwaltung von Ereignismetadaten.
Windows-Ereignissammlung		X		Systemmeldungen werden protokolliert und können im Fehlerfall ausgewertet werden. Besteht der Bedarf an einer Nachvollziehbarkeit der stattgefundenen Aktionen, darf dieser Dienst nicht deaktiviert werden.
Windows-Farbsystem		X		Dieser Service ist für die Einbindung fremder Farbsysteme notwendig. Werden Grafikanwendungen verwendet, so darf dieser Dienst nicht deaktiviert werden.
Windows-Fehlerberichterstattungsdienst			X	Dieser Dienst ermöglicht das Versenden von Berichten zu Systemfehlern an Microsoft.
Windows-Firewall	X			Solange keine andere Filter-Anwendung (lokale Firewall) verwendet wird, trägt dieser Dienst zum Schutz des Computers bei, indem der Zugriff durch nicht autorisierte Benutzer auf den Computer über das Internet bzw. ein Netzwerk verhindert wird.
Windows-Remoteverwaltung (WS-Verwaltung)		X		Dieser Dienst ist erforderlich, wenn WMI-Abfragen im Netzwerk verwendet werden.
Windows-Sicherung		X		Stellt die Funktion der Windows-eigenen Backup- und Wiederherstellung zur Verfügung. Wird eine andere Backup-Lösung verwendet, so kann dieser Dienst deaktiviert werden.
Windows-Sofortverbindung - Konfigurationsregistrierungsstelle		X		Erleichtert die Einrichtung von WLAN. Wird kein WLAN verwendet, so kann dieser Dienst deaktiviert werden.
Windows-Verwaltungsinstrumentation	X			Bietet eine standardmäßige Schnittstelle und Objektmodell zum Zugreifen auf Verwaltungsinformationen über das Betriebssystem, Geräte, Anwendungen und Dienste. Die meiste Windows-basierte Software kann nicht ordnungsgemäß ausgeführt werden, falls dieser Dienst beendet wird.
Windows-Zeitgeber	X			Dieser Dienst ist für die automatische Einstellung der Uhrzeit über das Netzwerk/Internet erforderlich.
WinHTTP-Web Proxy Auto-Discovery-Dienst		X		Werden automatische Proxy-Konfigurationen im Netzwerk erkannt, so werden diese für die entsprechenden Dienste (z. B. Http, Ftp) geladen. Wird eine statische Proxy-Konfiguration im APC eingetragen, so kann der Dienst deaktiviert werden.
WMI-Leistungsadapter		X		Dieser Dienst wird wie die Windows-Remoteverwaltung für WMI-Abfragen über das Netz verwendet.
WWAN - automatische			X	Wird nur für mobile Breitbandgeräte benötigt und

Dienst	*not-wendig*	*optional*	*nicht not-wendig*	*Begründung*
Konfiguration				kann daher deaktiviert werden.
Zertifikatverteilung		X		Wird für die Verwaltung von Zertifikaten auf Smartcards benötigt. Werden Smartcards, die Zertifikate enthalten verwendet (z. B. NPA, Bankkarte), so darf dieser Dienst nicht deaktiviert werden.
Zugriff auf Eingabegeräte		X		Ermöglicht die Ansteuerung von sog. Hot-Keys welche auf Eingabegeräten (z. B. Tastaturen, Fernbedienungen) vorhanden sind.) Werden spezielle Funktionstasten benötigt, darf dieser Dienst nicht deaktiviert werden.

Tabelle 15: Windows Dienste für den Betrieb des Minimalsystems

4.3.4 Optionale Deaktivierung

Nachfolgend werden in diesem Abschnitt die Dienste beschrieben, bei denen eine Deaktivierung empfohlen wird. Bei der Deaktivierung der optionalen Dienste ist die Funktionsfähigkeit der unter Abschnitt 2.5 genannten zusätzlichen Komponenten gewährleistet. Die Deaktivierung der Dienste kann je nach Anforderungen durch die Organisation oder weiteren zusätzlichen Anwendungen nicht sinnvoll sein und sollte daher auf Abhängigkeiten geprüft werden. Hierzu kann die Beschreibung aus dem Abschnitt zur Entscheidungsfindung herangezogen werden.

4.3.4.1 ActiveX-Installer (AxInstSV)

R

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\AxInstSV`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

G

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.4.2 Anmeldeinformationsverwaltung

R

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\VaultSvc`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

G

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.3 Anwendungserfahrung

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\AeLookupSvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.4 Automatische Konfiguration (verkabelt)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\dot3svc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell

Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.5 Automatische WLAN-Konfiguration

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Wlansvc

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

4.3.4.6 BitLocker-Laufwerkverschlüsselungsdienst

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\BDESVC

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.4.7 Blockebenen-Sicherungsmodul

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\wbengine

Name	Start
Typ	REG_DWORD

Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.4.8 Bluetooth-Unterstützungsdienst

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\bthserv`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.4.9 BranchCache

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\PeerDistSvc`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.4.10 Defragmentierung

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\defragsvc`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

`< DC2008R2_GPO_HÄRTUNG >`

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.11 Designs

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Themes`

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

4.3.4.12 Distributed Transaction Cordinator

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSDTC`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.13 Erkennung interaktiver Dienste

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\UI0Detect

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.14 IKE- und AuthIP Ipsec-Schlüsselerstellungsmodule

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\IKEEXT

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.15 Konfiguration für Remotedesktops

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SessionEnv`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

`< DC2008R2_GPO_HÄRTUNG >`

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.16 Microsoft-Softwareschattenkopie-Anbieter

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\swprv`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

`< DC2008R2_GPO_HÄRTUNG >`

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.17 Offlinedateien

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CscService

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

4.3.4.18 Remotedesktopdienste

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TermService

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.19 Richtlinie zum Entfernen der Smartcard

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SCPolicySvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.20 RPC-Locator

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RpcLocator

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.21 Sekundäre Anmeldung

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\seclogon

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell

Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.22 Sitzungs-Manager für Desktopfenster-Manager

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\UxSms

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.23 Smartcard

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SCardSvr

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.24 SSTP-Dienst

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SstpSvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.25 Superfetch

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SysMain

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.26 TPM-Basisdienste

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TBS

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.27 Verbessertes Windows-Audio/Video-Streaming

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\QWAVE

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.4.28 Verschlüsselung des Dateisystem (EFS)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\EFS

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.29 Windows Presentation Foundation-Schriftartcache 3.0.0.0

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\FontCache3.0.0.0

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.30 Windows-Bilderfassung (WIA)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\StiSvc

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

4.3.4.31 Windows-Dienst für Schriftartencache

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\FontCache

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.32 Windows-Ereignissammlung

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Wecsvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.33 Windows-Farbsystem

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WcsPlugInService

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.34 Windows-Remoteverwaltung (WS-Verwaltung)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WinRM

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.35 Windows-Sicherung

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SDRSVC

Name	Start

Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.36 Windows-Sofortverbindung - Konfigurationsregistrierungsstelle

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\wcncsvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.4.37 WinHTTP-Web Proxy Auto-Discovery-Dienst

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WinHttpAutoProxySvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell

Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.38 Zertifikatverteilung

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CertPropSvc

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.4.39 Zugriff auf Eingabegeräte

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\hidserv

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert

Neuer Wert	Deaktiviert

4.3.5 Nicht notwendige Dienste

Nachfolgend werden in diesem Abschnitt die Dienste beschrieben, die weitestgehend zur Herstellung eines gehärteten Betriebssystems deaktiviert werden können. Die Deaktivierung der Dienste kann je nach Anforderung der Organisation oder den zusätzlichen Anwendungen evtl. nicht sinnvoll sein. Daher ist eine Überprüfung auf eventuell bestehende Abhängigkeiten durchzuführen.

Die nachfolgend aufgelisteten „neuen Werte“ der START-Parameter sind einzustellen.

4.3.5.1 Adaptive Helligkeit

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SensrSvc`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.2 Anschlussumleitung für Terminaldienst im Benutzermodus

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\UmRdpService`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

`< DC2008R2_GPO_HÄRTUNG >`

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.3 Benachrichtigungsdienst für Systemereignisse

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SENS

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.4 Computerbrowser

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\bowser

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.5 Diagnosediensthost

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WdiServiceHost

Name	Start

Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.6 Diagnoserichtliniendienst

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\DPS

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.7 Diagnosesystemhost

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WdiSystemHost

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.8 Fax

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Fax

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

Anmerkung: Wurde dieser Dienst wie bereits im vorherigen Kapitel beschrieben bei der Härtung der Windows-Komponenten entfernt, ist der hier dargestellte Registry-Eintrag nicht vorhanden.

4.3.5.9 Funktionssuchanbieter-Host

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\fdPHost

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.10 Funktionssuche-Ressourcenveröffentlichung

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\FDResPub

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.11 Gatewaydienst auf Anwendungsebene

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ALG

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.12 Gemeinsame Nutzung der Internetverbindung

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.13 Heimnetzgruppen-Anbieter

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\HomeGroupProvider

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.14 Heimnetzgruppen-Listener

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\HomeGroupListener

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.15 IP-Hilfsdienst

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\iphlpsvc`

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

`< DC2008R2_GPO_HÄRTUNG >`

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.16 KtmRm für Distributed Transaction Coordinator

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\KtmRm`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

`< DC2008R2_GPO_HÄRTUNG >`

Default-Wert	Nicht definiert

Neuer Wert	Deaktiviert

4.3.5.17 Leistungsindikator-DLL-Host

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\perfhost`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

`< DC2008R2_GPO_HÄRTUNG >`

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.18 Leistungsprotokolle und -warnungen

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\pla`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

`< DC2008R2_GPO_HÄRTUNG >`

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.19 Media Center Extender-Dienst

Dieser Dienst ist per Default deaktiviert.

4.3.5.20 Microsoft iSCSI-Initiator-Dienst

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSiSCSI

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.21 Net.Tcp-Portfreigabedienst

Dieser Dienst ist per Default deaktiviert.

4.3.5.22 Parental Controls

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WPCSvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.23 Peer Name Resolution-Protokoll

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\PNRPsvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.24 Peernetzwerk-Gruppenzuordnung

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\p2psvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.25 Peernetzwerkidentitäts-Manager

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\p2pimsvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell

Neuer Wert	Deaktiviert

4.3.5.26 PnP-X-IP-Busenumerator

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\IPBusEnum

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.27 PNRP-Computernamenveröffentlichungs-Dienst

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\PNRPAutoReg

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.28 Programmkompatibilitäts-Assistent-Dienst

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\PcaSvc

Name	Start
Typ	REG_DWORD

Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

4.3.5.29 RAS-Verbindungsverwaltung

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RasMan`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

`< DC2008R2_GPO_HÄRTUNG >`

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.30 Remoteregistrierung

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RemoteRegistry`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.31 Routing und RAS

Dieser Dienst ist per Default deaktiviert.

4.3.5.32 Server

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.33 Shellhardwareerkennung

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ShellHWDetection

Name	Start
Typ	REG_DWORD
Default-Wert	2
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Automatisch
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.34 SNMP-Trap

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SNMPTRAP

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.35 SSDP-Suche

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SSDPSRV

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.36 Tablet PC-Eingabedienst

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TabletInputService

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.37 Telefonie

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TapiSrv

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.38 Überwachung verteilter Verknüpfungen (Client)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TrkWks

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.39 Unterstützung in der Systemsteuerung unter Lösungen für Probleme

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\wercplsupport

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.40 UPnP-Gerätehost

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\upnphost

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.41 Verbindungsschicht-Topologieerkennungs-Zuordnungsprogramm

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\lltdsvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.42 Verwaltung für automatische RAS-Verbindung

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RasAuto

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.43 Virtueller Datenträger

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vds

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

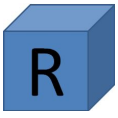
Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.44 Volumenschattenkopie



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\VSS

Name	Start
Typ	REG_DWORD
Default-Wert	3n
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.45 WebClient

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WebClient

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.46 Windows CardSpace

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\idsvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.47 Windows Media Center-Empfängerdienst

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ehRecvr

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.48 Windows Media Center-Planerdienst

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ehSched`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.49 Windows Media Player-Netzwerkfreigabedienst

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WMPNetworkSvc`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.50 Windows-Biometriedienst

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WbioSrvc`

Name	Start
Typ	REG_DWORD

Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

4.3.5.51 Windows-Fehlerberichterstattungsdienst

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WerSvc`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

`< DC2008R2_GPO_HÄRTUNG >`

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.52 WMI-Leistungsadapter

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\wmiApSrv`

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

< DC2008R2_GPO_HÄRTUNG >

Default-Wert	Nicht definiert
Neuer Wert	Deaktiviert

4.3.5.53 WWAN - Automatische Konfiguration

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WwanSvc

Name	Start
Typ	REG_DWORD
Default-Wert	3
Neuer Wert	4

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp

Default-Wert	Manuell
Neuer Wert	Deaktiviert

5 Wartung

Das in Abschnitt 3 installierte und in Abschnitt 4 gehärtete Windows 7 dient als Referenzsystem für die Erstellung eines Images. Dieses Image dient wiederum als Basis für die Installation weiterer APCs. In diesem Abschnitt werden Erstellung und Wartung eines Images beschrieben.

Die Erstellung eines Images und das Ausrollen auf weitere APCs sind mit einer Vielzahl von Werkzeugen möglich. Dieses Dokument beschreibt die Image-Erstellung mit Hilfe von Microsoft-Werkzeugen, also ohne Softwareverteilung eines Drittherstellers.

Für Vertiefungen dieses Themas sowie für die Umsetzung spezifischer individueller Anforderungen wird empfohlen, die folgende Microsoft TechNet Seite zu nutzen: http://technet.microsoft.com/de-de/. Für Vertiefungen der Softwareverteilung von Microsoft Produkten wird die Literatur über Microsoft Werkzeuge „Deployment-Werkzeuge für Windows 7 (AIK, MDT)“ sowie Operating-System-Deployment (OSD) und Komponenten von SCCM (System Image Manager, ImageX) empfohlen.

Da es sich bei einer Image-Installation um ein identisches Abbild des Referenzsystems handelt, sind nach einer Image-Installation bestimmte individuelle Anpassungen am APC vorzunehmen. Es wird empfohlen, das Referenzsystem zu generalisieren und APC-spezifische Anpassungen nach der Image-Installation vorzunehmen. Hierdurch erhält man eine weitgehende Unabhängigkeit des Images von APC-spezifischen Konfigurationsparametern. Folgende Parameter sind anzupassen:

- Computername / Computerbeschreibung
- Security Identifier (SID)
- Aktuelle Windows-Updates
- Aktuelle Antivirenschutzprogramm (Scan-Engine und Pattern-File)
- ggf. Windows-Aktivierung
- ggf. Aufnahme in einer Windows Domäne / Windows Arbeitsgruppe
- ggf. Anpassung der Hardware-Informationen

Abschnitt 5.1 beschreibt die Image-Erstellung. Die Abschnitte 5.2, 5.3 und 5.3.2 gehen auf die Wiederherstellung eines Images ein.

Wird eine grundlegende Veränderung am Betriebssystem nach der Installation oder zur Betriebslaufzeit vorgenommen, wie beispielsweise die Installation von Service Packs oder der Aktualisierung von Treibern, so sind diese in das Referenzsystem einzubinden. Dies wird in Abschnitt 5.4 beschrieben.

Veränderungen am Referenzsystem sollten in Konfigurationsdatenbanken revisionssicher hinterlegt werden. Abbildung 2.13 illustriert den Arbeitsablauf zur Erstellung und Wartung von Abbildern.

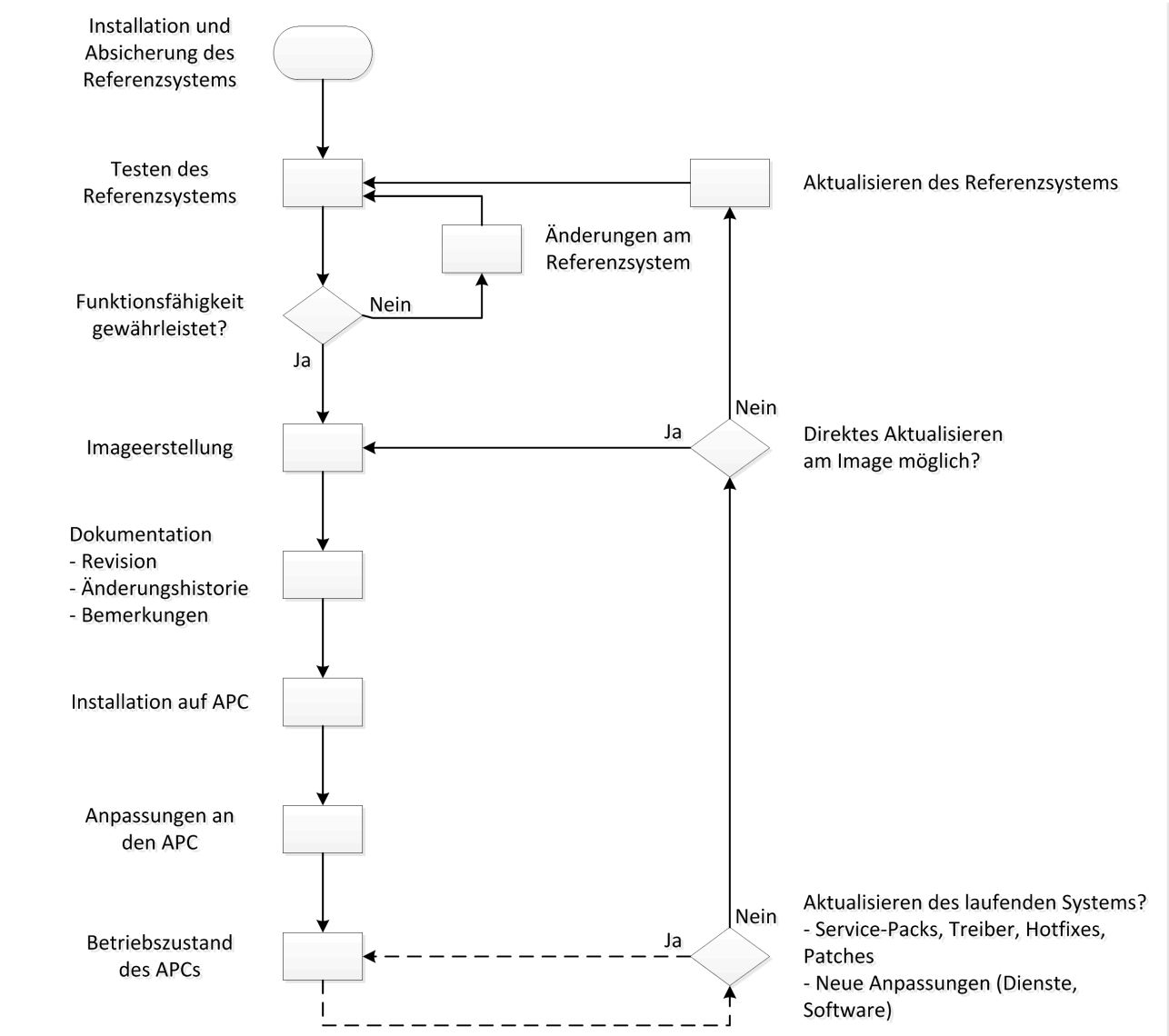


Abbildung 5.1: Schaubild zur Erstellung und Pflege eines Referenzsystems

5.1 Erstellung eines Abbildes

In diesem Abschnitt wird die konkrete Vorgehensweise zur Erstellung eines funktionalen Abbilds eines Referenzsystems beschrieben. Mit Hilfe des Programms `Sysprep`[93] können Benutzer- und APC-spezifische Einstellungen aus dem Referenzsystem entfernt werden.

Um von dem Referenzsystem ein Image zu erstellen, ist das Referenzsystem mit einem Hilfs-Betriebssystem zu starten. Hierfür bietet sich das Microsoft Windows Preinstallation Environment (WinPE) an, das Bestandteil des Windows Automated Installation Kit (WAIK) für Windows 7 ist [94]. Für die Erstellung von Windows Abbildern lässt sich beispielsweise das Programm `ImageX.exe`

93 http://technet.microsoft.com/de-de/library/cc721940%28WS.10%29.aspx
94 http://www.microsoft.com/downloads/de-de/details.aspx?FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34&pf=true

verwenden, das ebenfalls Bestandteil des WAIK ist. Mit der Version WAIK 7 SP1[95] wurde die Version WinPE 3.1 erstellt, die zusätzliche optionale Komponenten wie beispielsweise Netzwerktreiber und Zusatzprogramme einbinden kann[96].

Insgesamt ergeben sich folgende Voraussetzungen für die Erstellung eines Systemabbildes:

- `ImageX.exe` zur Erzeugung der Windows-Abbildungsdatei (WIM-Datei). Dieses Programm ist als zusätzliche Komponente im WinPE 3.1 einzubinden.
- `sysprep.exe` zur Generalisierung des Referenzsystems. Dieses Programm ist als zusätzliche Komponente im WinPE 3.1 einzubinden.
- Netzwerktreiber für den APC. Diese sind zusätzlich im WinPE 3.1 einzubinden.
- Speicherort oder Medium für das Windows-Abbild. Hierbei sind zwei Varianten möglich:
  - Speicherung auf einer separaten Festplatte.
  - Speicherung auf einem freigegebenen Netzlaufwerk. (Auf dem Server müssen Berechtigungs- und Netzzugriff gewährleistet sein sowie der APC eine gültige IP besitzen). Mit dem Befehl `net use` lassen sich Netzwerkfreigaben mounten. Beispielsweise wird die Freigabe `ISO` von dem Server `FILE01` an dem Laufwerksbuchstaben `I` durch den Domänen Administrator Account der Domäne `intern.local` gebunden.

```
net use I: \\FILE01\ISO /USER:Administrator@intern.local
```

Vorgehensweise zur Windows-Abbild Erstellung und Speicherung

1. Generalisierung des Referenzsystems mit dem Befehlszeilenprogramm `sysprep.exe`[97]

   i. Start → Ausführen → cmd → Rechtsklick → „Als Administrator ausführen“ → In das Verzeichnis „C:\Windows\System32\sysprep\“ wechseln → Ausführen von „sysprep.exe“. Es erscheint Folgendes Fenster (s. h. Abbildung 5.2).

   Bei der Auswahl der Systembereinigungsaktion gibt es zwei Auswahl-Möglichkeiten:

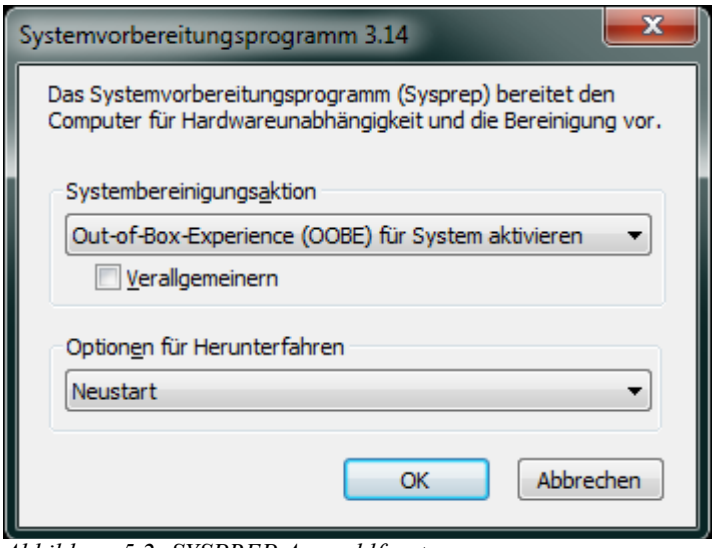


Abbildung 5.2: SYSPREP Auswahlfenster

95 http://www.microsoft.com/downloads/de-de/details.aspx?FamilyID=0AEE2B4B-494B-4ADC-B174-33BC62F02C5D&pf=true#QuickDetails
96 http://technet.microsoft.com/de-de/library/dd744533%28WS.10%29.aspx
97 http://technet.microsoft.com/de-de/library/ee523217%28WS.10%29.aspx

a) Out-of-Box-Experience (OOBE) für System aktivieren

Hierbei wird der der Rechner nach einem Neustart komplett generalisiert und entkernt. Auch Treiber werden neu installiert. Der Benutzer muss dann bei der Erstanmeldung Benutzer- und APC-spezifische Einstellungen vornehmen wie z. B. Sprache, Gebietsschema, etc. Der Befehl kann auch mit einem Softwareschalter ausgeführt werden: `sysprep.exe /oobe`. Mit dem Befehl `sysprep.exe /generalize` wird das System verallgemeinert. Die Ausführung dieser Funktion ist identisch mit der Aktivierung des optional zu setzenden Hakens „Verallgemeinern".

b) Systemüberwachungsmodus aktivieren

Mit dieser Einstellung können Einstellungen (z. B. Treiberinstallation bei einem Hardwaretausch, Updates oder Softwareinstallationen) an einem APC vorgenommen werden, der mit einem Referenzsystem initial installiert wurde. Der Befehl kann auch mit einem Softwareschalter ausgeführt werden: `sysprep.exe /audit`. Mit dem Befehl `sysprep.exe /generalize /audit` wird das System verallgemeinert. Nach der erfolgreichen Aktualisierung wird das System mit `sysprep.exe /oobe` wieder versiegelt (siehe auch Abschnitt 5.4).

Weiterhin gibt es die drei folgenden Optionen zu den beiden Systembereinigungsaktionen:

i. Neustart – Führt einen direkten Neustart des APC durch und aktiviert nach dem Neustart eine der beiden ausgewählten Systembereinigungsaktionen.

ii. Herunterfahren – Fährt den APC herunter und schaltet ihn ggf. ab. Die Systembereinigungsaktion wird nach dem nächsten Start des APC durchgeführt.

iii. Beenden – Das Systembereinigungsprogramm wird beendet, ohne das ein Neustart oder ein Herunterfahren durchgeführt wurde.

Beim Starten von `sysprep.exe` kann eine erstellte Antwortdatei für eine unbeaufsichtigte Installation als Softwareschalter mitgeben werden: `sysprep.exe /unattend:Antwortdatei.mxl`. In Abschnitt 5.3.2 wird auf die Erstellung einer Antwortdatei eingegangen.

2. Booten des Referenzsystems mit einem angepassten Windows PE System. Abbildung 5.3 zeigt den APC nach einem Boot mit WinPE.[98]

98 http://technet.microsoft.com/de-de/library/dd744320%28WS.10%29.aspx

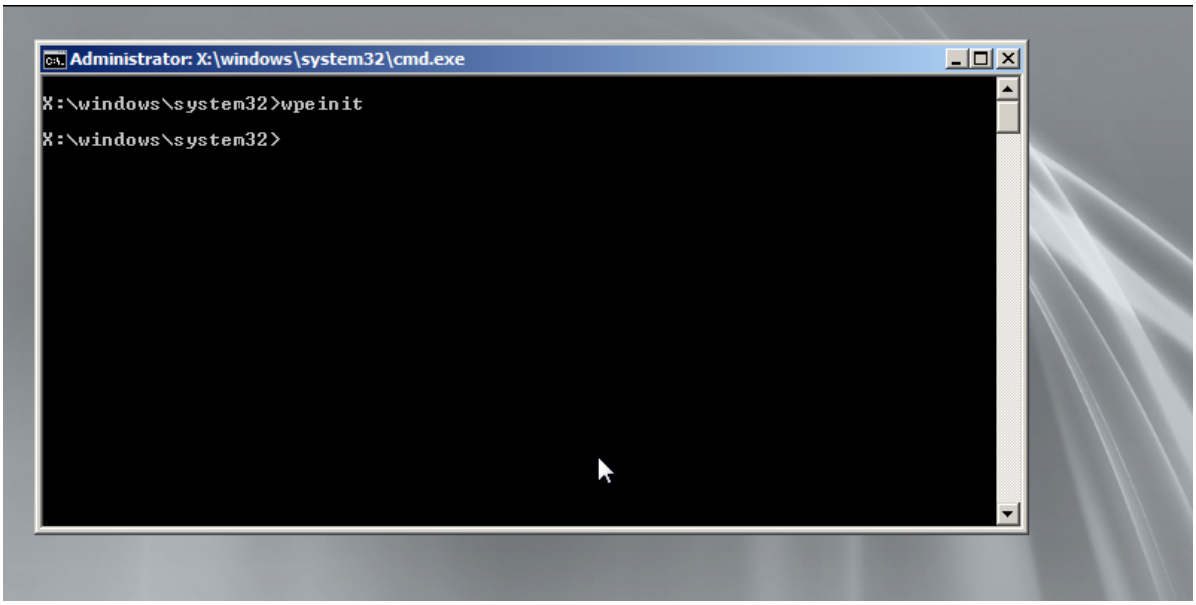


Abbildung 5.3: Boot des APC mit WinPE

3. Zuordnung der Festplattenlaufwerke mit dem Programm `Diskpart.exe`

   Auflistung der angeschlossenen Festplatten und der logischen Laufwerke:

   i. Mit dem Befehl `list disk` werden die an dem APC angeschlossenen physischen Festplatten angezeigt. In Abbildung 5.4 ist der Datenträger 0 die Systemfestplatte des Referenzsystems und der Datenträger 1 eine externe Festplatte zur Speicherung des Images des Referenzsystems.

```
DISKPART> list disk

  Datenträger ###  Status         Größe    Frei     Dyn  GPT
  ---------------  -------------  -------  -------  ---  ---
  Datenträger 0    Online           15 GB  1024 KB
  Datenträger 1    Online           40 GB  1024 KB
```

Abbildung 5.4: Auflistung der physischen Platten

   ii. Mit dem Befehl `list volume` werden die an dem APC erkannten logischen Laufwerke angezeigt. In Abbildung 5.5 werden die Laufwerke den Laufwerksnamen zugeordnet. Wird das logische Laufwerk des Referenzsystem nicht mit einem Laufwerksbuchstaben aufgelistet, muss dieses manuell gemountet werden. Dies sind die Schritte 4 – 7. Wird das Referenzsystem einwandfrei gemountet, ist mit Schritt 8 fortzufahren.

```
DISKPART> list volume

  Volume ###  Bst  Bezeichnung  DS     Typ          Größe    Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     F   CD_ROM       CDFS   CD           161 MB  Fehlerfre
  Volume 1     C   System-rese  NTFS   Partition    100 MB  Fehlerfre
  Volume 2     E                NTFS   Partition     14 GB  Fehlerfre
  Volume 3     D   IMAGE        NTFS   Partition     39 GB  Fehlerfre
```

Abbildung 5.5: Auflisten der Laufwerke

4. Mit dem `select disk=0` wird die Systemfestplatte des Referenzsystems ausgewählt – siehe Abbildung 5.6.

```
DISKPART> select disk=0

Datenträger 0 ist jetzt der gewählte Datenträger.
```

Abbildung 5.6: Auswahl der Systemfestplatte

5. Mit dem `list partition` werden die Partitionen der Systemfestplatte angezeigt. In Abbildung 5.7 sind für die Systemfestplatte 0 zwei Partitionen ersichtlich. Zum einen die Partition 1, die eine systemreservierte Partition für Windows 7 darstellt und zum anderen die Partition 2, die das Windows Betriebssystem enthält.

```
DISKPART> list partition

  Partition ###  Typ              Größe    Offset
  -------------  ---------------  -------  -------
  Partition 1    Primär            100 MB  1024 KB
  Partition 2    Primär             14 GB   101 MB
```

Abbildung 5.7: Auflisten der Partitionen des Referenzsystems

6. Auswahl der Partition von der ein Abbild erstellt werden soll mit dem Befehl `select partition=1`. Siehe Abbildung 5.8.

```
DISKPART> select partition=1

Partition 1 ist jetzt die gewählte Partition.
```

Abbildung 5.8: Auswahl der Partition

7. Ein Laufwerksbuchstabe ist mit dem Befehl `assign letter=Z` nur zu vergeben, wenn dem Laufwerk noch kein Laufwerksbuchstabe zugeordnet ist. Dies ist in Abbildung 5.9 dargestellt.

```
DISKPART> assign letter=Z

Der Laufwerkbuchstabe oder der Bereitstellungspunkt wurde zugewiesen.
```

Abbildung 5.9: Zuweisung des Laufwerksbuchstaben

8. Mit dem Befehl `exit` wird das Dienstprogramm `DISKPART` beendet.
9. Es ist das Imageerstellungsprogramm `ImageX.exe` zu starten. Dafür ist in das entsprechende Verzeichnis zu wechseln, in dem sich das Programm befindet.
10. Mit dem Befehl `imagex /capture E:\ D:\Windows_7_Referenz-system_System.wim "BSI_Referenzsystem"` wird das Betriebssystem als Image erstellt (s. Abbildung 5.10).

    Hinweis: Von der Systempartition muss kein Windows-Abbild erstellt werden, da ein neuer Bootmanager Bereich erstellt werden kann (siehe Abbildung).

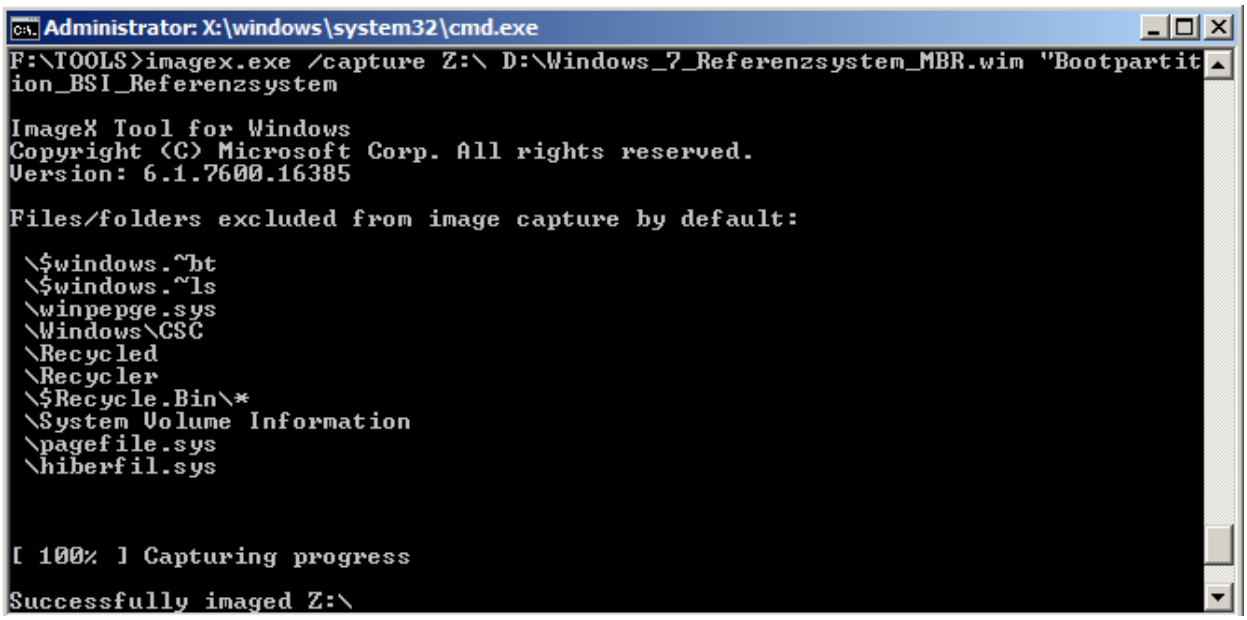


Abbildung 5.10: Erstellung des Abbilds für die Systempartition

5.2 Wiederherstellung des Windows-Abbilds

Um ein Windows-Abbild des Referenzsystems auf weiteren APCs zu installieren, wird der Windows Automated Installation Kit für Windows 7 (WAIK) benötigt, sowie eine formatierte Festplatte des Ziel-APCs und ein bootfähiges Windows PE 3.1[99] mit folgenden Komponenten:

- `ImageX.exe` für das Rückspielen der Windows-Abbildungsdatei (WIM-Datei). Dieses Programm ist als zusätzliche Komponente im WinPE 3.1 einzubinden.
- `sysprep.exe`, falls das Referenzsystem noch nicht generalisiert wurde. Dieses Programm ist als zusätzliche Komponente im WinPE 3.1 einzubinden.
- Netzwerktreiber für den APC (Netzwerkzugriff zum Systemabbild. Diese sind zusätzlich ins WinPE 3.1 einzubinden.

Speicherort oder Medium für das Windows-Abbild bereitstellen. Es sind drei Varianten möglich:

1. Wiederherstellung von einer separaten Festplatte.
2. WinPE Medium mit dem Windows-Abbild (z. B. CD/ DVD/ USB-Stick).
3. Wiederherstellung von einer Netzwerkfreigabe. (Auf dem Server müssen Berechtigungs- und Netzzugriff gewährleistet sein, der APC muss eine gültige IP erhalten). Mit dem Befehl `net use` lassen sich Netzwerkfreigaben mounten. Beispielsweise wird die Freigabe ISO von dem Server `FILE01` an dem Laufwerksbuchstaben `I` durch den Domänen Administrator Account der Domäne `intern.local` gebunden:
   `net use I: \\FILE01\ISO /USER:Administrator@intern.local`

Vorgehensweise zur Windows-Abbild Wiederherstellung

1. Booten des APC mit einem angepassten Windows PE System.
2. Mit dem `select disk=0` wird die Systemfestplatte des zu installierenden APC ausgewählt (siehe Abbildung Fehler: Referenz nicht gefunden). Falls noch keine aktive und formatierte Partition in dem APC erstellt wurde, dann kann dies über das Programm `DISKPART` durchgeführt werden. Falls der APC eine formatierte Festplatte besitzt, ist mit Punkt 8 fortzufahren.

```
DISKPART> list disk

  Datenträger ###  Status         Größe    Frei     Dyn  GPT
  ---------------  -------------  -------  -------  ---  ---
  Datenträger 0    Online           20 GB    20 GB
  Datenträger 1    Online           15 GB      0 B

DISKPART> list volume

  Volume ###  Bst  Bezeichnung  DS     Typ          Größe    Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D   CD_ROM       CDFS   CD           161 MB  Fehlerfre
  Volume 1     C                NTFS   Partition     14 GB  Fehlerfre

DISKPART> select disk=0

Datenträger 0 ist jetzt der gewählte Datenträger.
```

Abbildung 5.11: Aktive Festplatte auswählen

99 http://technet.microsoft.com/de-de/library/dd744548%28WS.10%29.aspx

3. Mit dem Befehl `create partition primary` wird eine primäre Partition erstellt. Hinweis: Es müssen mindestens zwei Partitionen erstellt werden. Zum einen für den reservierten Windows Bootmanager (Speichergröße: 150 MB) und zum anderen für das Betriebssystem. Mit dem Befehl `list partition` kann man sich die erstellten Partition anzeigen lassen (siehe Abbildung 5.12).
   - Erstellung der Systempartition: `create partition primary size=100`
   - Erstellung der Windowspartition: `create partition primary`

```
DISKPART> list partition

  Partition ###  Typ              Größe    Offset
  -------------  ---------------  -------  -------
  Partition 1    Primär            100 MB  1024 KB
* Partition 2    Primär             19 GB   151 MB
```

Abbildung 5.12: Auflisten der primären Partition

4. Beide neu erstellten Partitionen sind als aktiv zu markieren (siehe Abbildung 5.13).
   - Auswahl einer Partition: `select partition=1`
   - Aktiv markieren: `active`

```
DISKPART> select partition=1

Partition 1 ist jetzt die gewählte Partition.

DISKPART> active

Die aktuelle Partition wurde als aktiv markiert.

DISKPART> select partition=2

Partition 2 ist jetzt die gewählte Partition.

DISKPART> active
```

Abbildung 5.13: Aktivierung der Partitionen

5. Mit dem Befehl `format` wird die in Punkt 4 erstellte Partition mit NTFS formatiert (siehe Abbildung 5.14). Der Befehl wird auf der zuletzt ausgewählten Partition angewendet.

```
DISKPART> format FS=NTFS LABEL="Betriebssystem" quick

  100 Prozent bearbeitet

DiskPart hat das Volume erfolgreich formatiert.

DISKPART> select partition=1

Partition 1 ist jetzt die gewählte Partition.

DISKPART> format FS=NTFS LABEL="MBR" quick

  100 Prozent bearbeitet

DiskPart hat das Volume erfolgreich formatiert.
```

Abbildung 5.14: Formatierung der Partition

6. Mit dem Befehl `list partition` wird der Zustand der logischen Laufwerke angezeigt (siehe Abbildung 5.15).

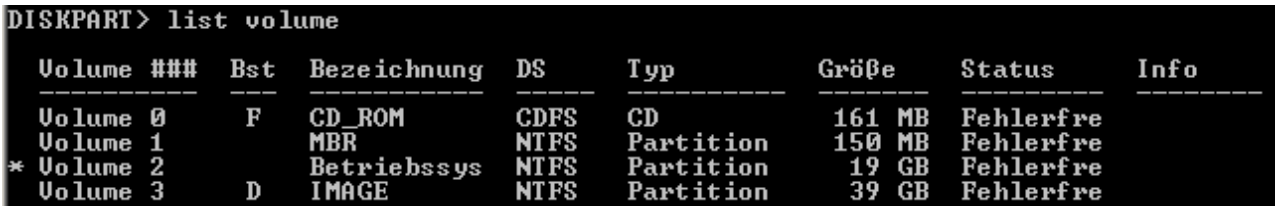


Abbildung 5.15: Überprüfung des Laufwerks

7. Wenn das ausgewählte Laufwerk (markiert mit einem Stern) noch nicht einem Laufwerksbuchstaben zugeordnet ist, dann wird dies mit Befehl `assign letter=C` durchgeführt (siehe Abbildung 5.16). Mit dem Befehl `exit` wird das Programm verlassen. Hinweis: Die Partition für den Bootmanager muss keinem Laufwerksbuchstaben zugeordnet werden.

Abbildung 5.16: Zuweisung eines Laufwerksbuchstaben

8. Die Wiederherstellung des Windows-Abbilds auf einem APC wird wie folgt durchgeführt: Mit dem Befehl `imagex /apply D:\Windows_7_Referenzsystem.wim 1 C:` wird das Abbild des Referenzsystem auf den Ziel-APC zurück gespielt. Dabei ist die Syntax des Befehls folgendermaßen zu lesen: `imagex /apply <Quelle> <Anzahl Images> <Ziel>`

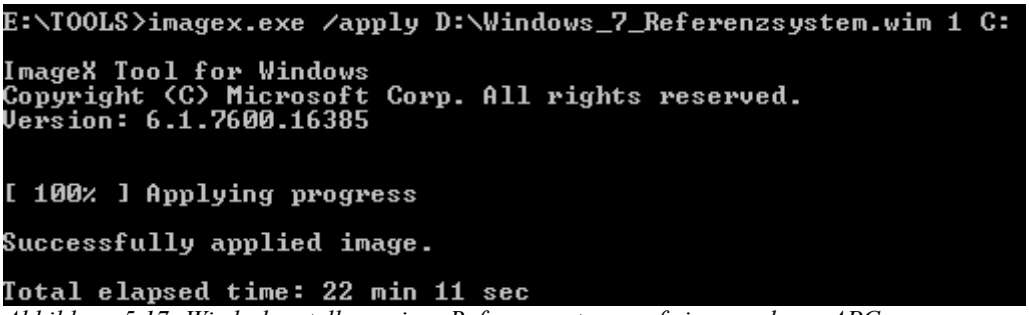


Abbildung 5.17: Wiederherstellung eines Referenzsystems auf einen anderen APC

9. Nach der erfolgreichen Wiederherstellung des Betriebssystems ist der Bootmanager neu zu installieren. Mit dem Befehl `bcdboot C:\windows` ist ein neuer Bootmanager in der aktiven Partition zu erstellen. Die Syntax des Befehls lässt sich wie folgt lesen: `bcdboot <Quelle>`. Die Quelle ist der wiederhergestellte Systemstamm des Betriebssystems. Hinweis: Damit ein neuer Bootmanager erstellt werden kann, müssen die Laufwerke aktiv sein (siehe Punkt 4). Beim ersten Boot kann der Bootmanager darauf hinweisen, dass das System nicht ordnungsgemäß herunter gefahren wurde. Um einen möglichen Schaden an dem Betriebssystem abzuwenden, startet das Betriebssystem zuerst mit einem „Windows Error Recovery“ Hinweis.

Durch die Auswahl von vier möglichen Bootoptionen kann der Benutzer Windows starten.

1. Safe Mode – Dies ist der abgesicherte Modus von Windows 7. Es werden nur die notwendigsten Treiber für Windows 7 geladen, die für ein eingeschränktes Arbeiten (z. B. Fehlersuche, Deinstallation von falschen Treibern, etc.) mit Windows 7 notwendig sind.

2. Safe Mode with Networking - Dies ist der Safe Mode mit geladenen Netzwerktreibern. Dieser eignet sich um lokale Daten des APC auf einer Netzwerkfreigabe zu sichern, falls dieser nicht mehr ordnungsgemäß startet.
3. Safe Mode with Command Prompt - Dies ist der Safe Mode von Windows 7 wobei nur eine CLI (Command Line Interface) gestartet wird, um Windows 7 zu verwalten.
4. Start Windows Normally - Windows 7 wird mit allen installierten Treibern sowie Softwarepaketen gestartet.

   Standardmäßig startet der Bootmanager nach einer Auswahlzeit von 30 Sekunden automatisch das Betriebssystem in dem Modus Start Windows Normally (s. Abbildung 5.18). Es bedarf eines manuellen Eingriffs des Benutzers, um auszuwählen, ob das System in einer der abgesicherten Umgebungen (Safe Mode) gestartet werden soll. Weiterhin besteht die Möglichkeit diesen Wiederherstellungsmodus für kommende Starts des Betriebssystems zu umgehen. Mit dem Befehl `bcdedit`[100] kann das Booten des Wiederherstellungsmodus für kommende Starts abgeschaltet werden. Der komplette Befehl lautet

   ```
   bcdedit /set {current} bootstatuspolicy ignoreallfailures
   ```

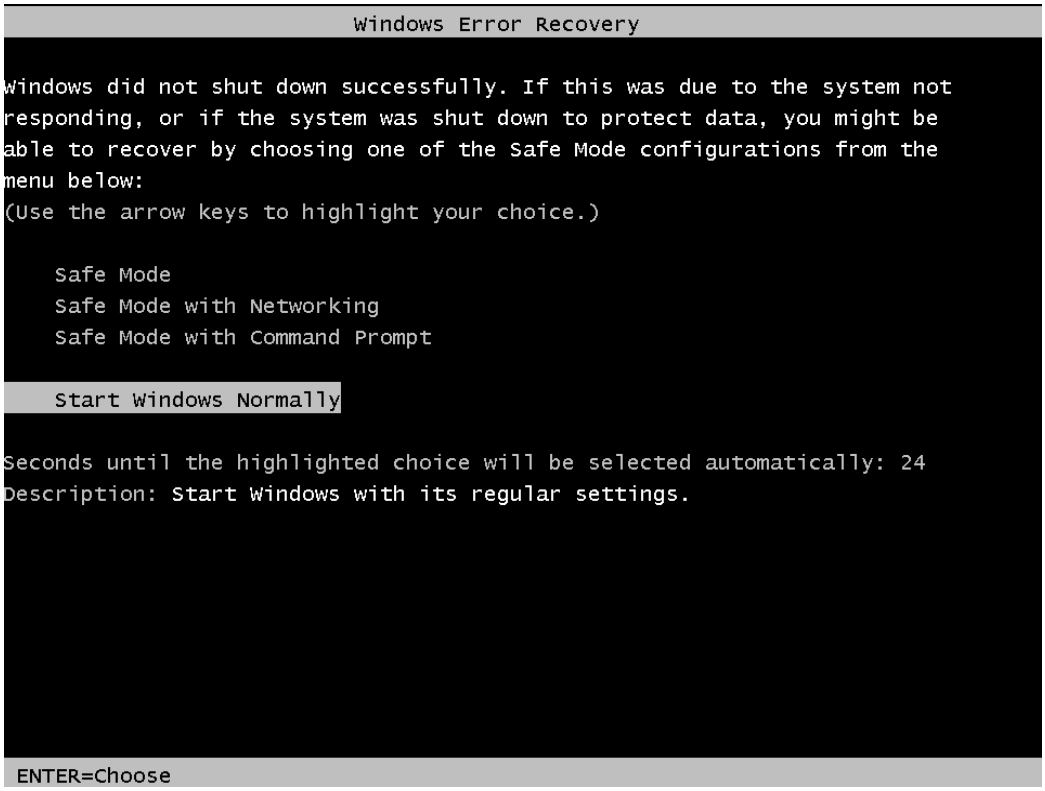


Abbildung 5.18: Bootmanager Meldung nach der Wiederherstellung

100 http://technet.microsoft.com/de-de/library/cc709667%28WS.10%29.aspx

5.3 Installation des Referenzsystem via Bereitstellungsdienst

Abschnitt 5.3.1 beschreibt die Installation des Referenzsystems mit Hilfe des Windows Bereitstellungsdiensts. Auf eine unbeaufsichtigte Installation mittels Antwortdatei wird in Abschnitt 5.3.2 eingegangen.

Folgende Voraussetzungen bestehen für eine unbeaufsichtigte, automatisierte Installation:

- Generalisierung des Referenzsystems (falls noch nicht durchgeführt)[101]
- Windows System Image Manager (Windows SIM)
- Windows Bereitstellungsdienst
- PXE-Boot, Netz- und Authentifizierungszugriff
- Erstellung einer Antwortdatei
- Zugriff auf das Referenzsystem

5.3.1 Einbindung des Referenzsystems

1. Nach der erfolgreichen Anmeldung auf dem Installationsserver, der als Bereitstellungsdienst zur Verfügung steht, wird wie gewohnt der Bereitstellungsdienst geöffnet.
2. Es wird der entsprechenden Server und der Ordner der „Installationsabbilder“ mit der entsprechenden „ImageGroup“ ausgewählt, der das Referenzsystem für die Verteilung bereitstellen soll.
3. Rechtsklick auf die „ImageGroup“ → „Installationsabbild hinzufügen“ → die Windows-Abbilddatei auswählen → „Weiter“ klicken → verfügbaren Abbilder auswählen
4. Zusammenfassung lesen und mit „Weiter“ bestätigen.
5. Überwachung des Prozess des Einbindens.
6. Aktuelle Übersicht und Zusammenfassung (Abbildung 5.19)

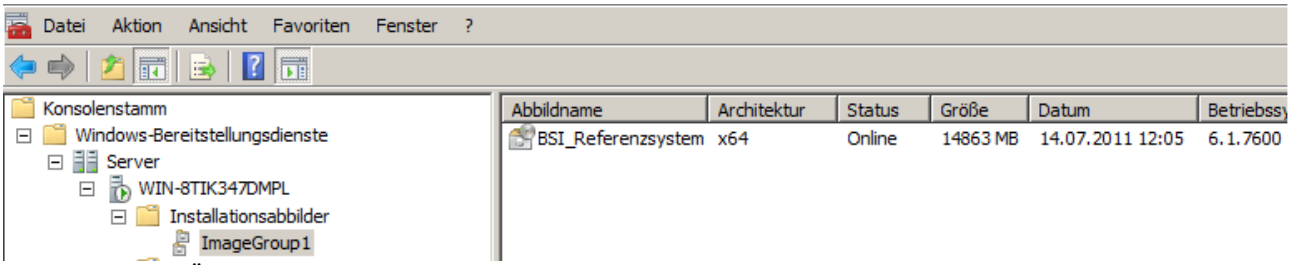


Abbildung 5.19: Übersicht der Abbilderstellung

101 http://technet.microsoft.com/de-de/library/dd799233%28WS.10%29.aspx und http://technet.microsoft.com/de-de/library/dd744392%28WS.10%29.aspx

5.3.2 Einbindung des Referenzsystems mit einer Antwortdatei

Für die Einbindung des Referenzsystems mit einer Antwortdatei, die für eine vollautomatische und unbeaufsichtigte Installation dienen kann, ist das Programm Windows System Image Manager und eine bestehende oder neu zu erstellende Antwortdatei notwendig.

1. Nach dem Starten des Windows System Image Manager ist das Referenzsystem als Windows-Abbild einzubinden (siehe Abbildung 5.20).

   Rechtsklick in „Windows-Abbild“ → „Windows-Abbild auswählen“ → Pfad zum Windows-Abbild auswählen.

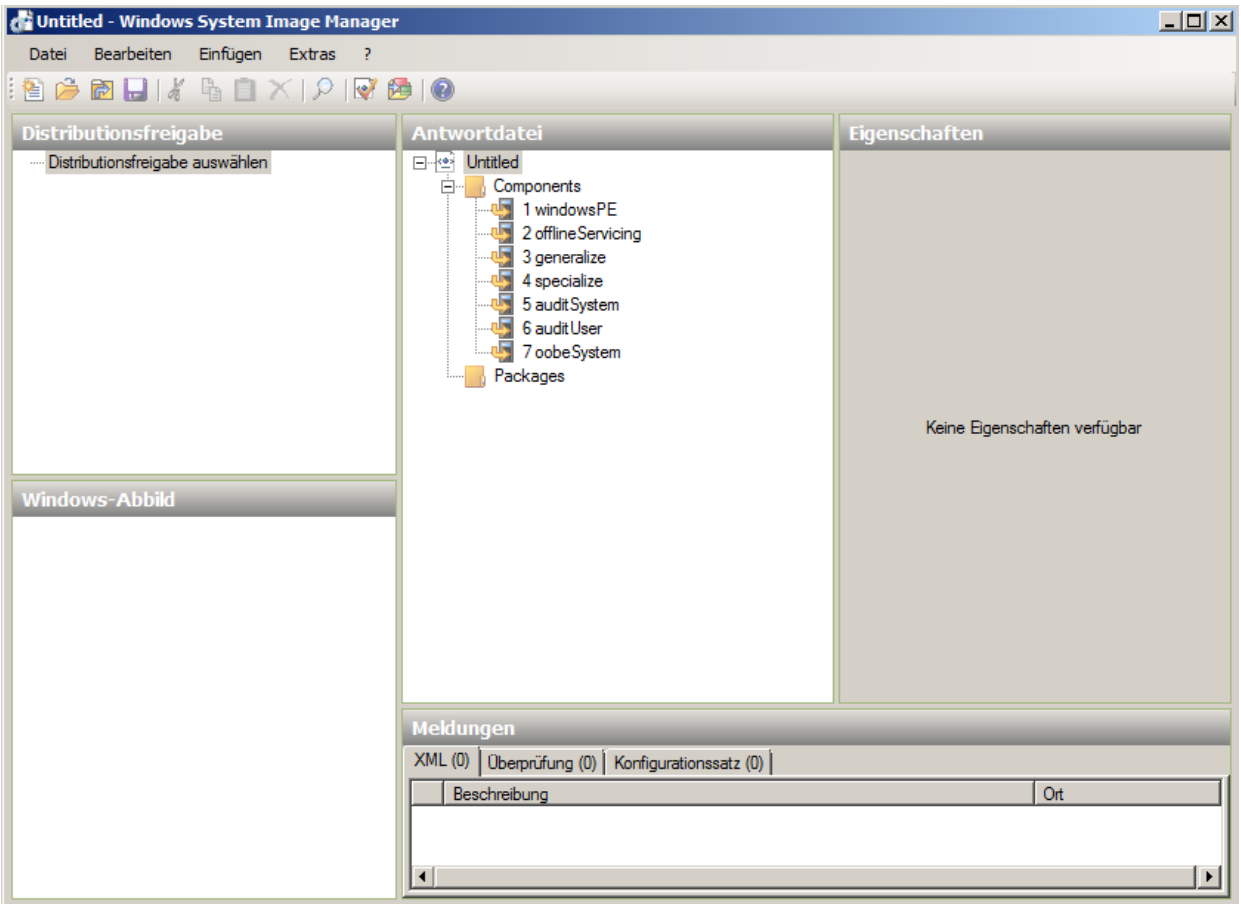


Abbildung 5.20: Windows-Abbild auswählen

2. Für die Einbindung des Windows-Abbilds ist die Erstellung entsprechender Katalogdateien notwendig (siehe Abbildung 5.21). Dafür ist der Vorgang mit „Ja“ zu bestätigen.

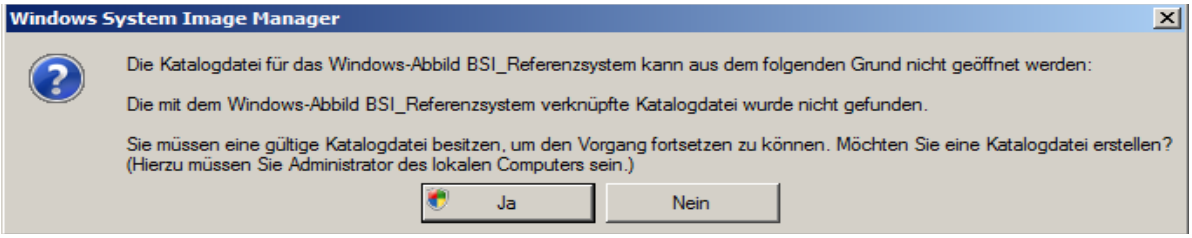


Abbildung 5.21: Erstellung der Katalogdateien

3. Um eine Antwortdatei anzulegen, wird in der Spalte „Antwortdatei“ durch Rechtsklick → „Neue Antwortdatei“ eine neue Antwortdatei erstellt.

4. Die Konfiguration der Antwortdatei wird in sieben unterschiedlichen Windows Setup-Konfigurationsphasen unterschieden. Weitergehende Informationen zu den Konfigurationsphasen sind der Seite http://technet.microsoft.com/de-de/library/cc749307%28WS.10%29.aspx zu entnehmen. Die Tabelle 16 enthält die grundlegenden Konfigurationsschritte einer Antwortdatei.
5. Die Antwortdatei wird nun im Bereitstellungsdienst hinterlegt (s. h. Abbildung 5.20): „Konsolenstamm“ → „Windows-Bereitstellungdienste → „Server“ → Mit Rechtsklick den Server auswählen → „Eigenschaften“ → „Client“ → Aktivieren von „Unbeaufsichtigte Installation aktivieren“ → Antwortdatei mit „Durchsuchen“ für die „x64-Architektur“ hinterlegen.

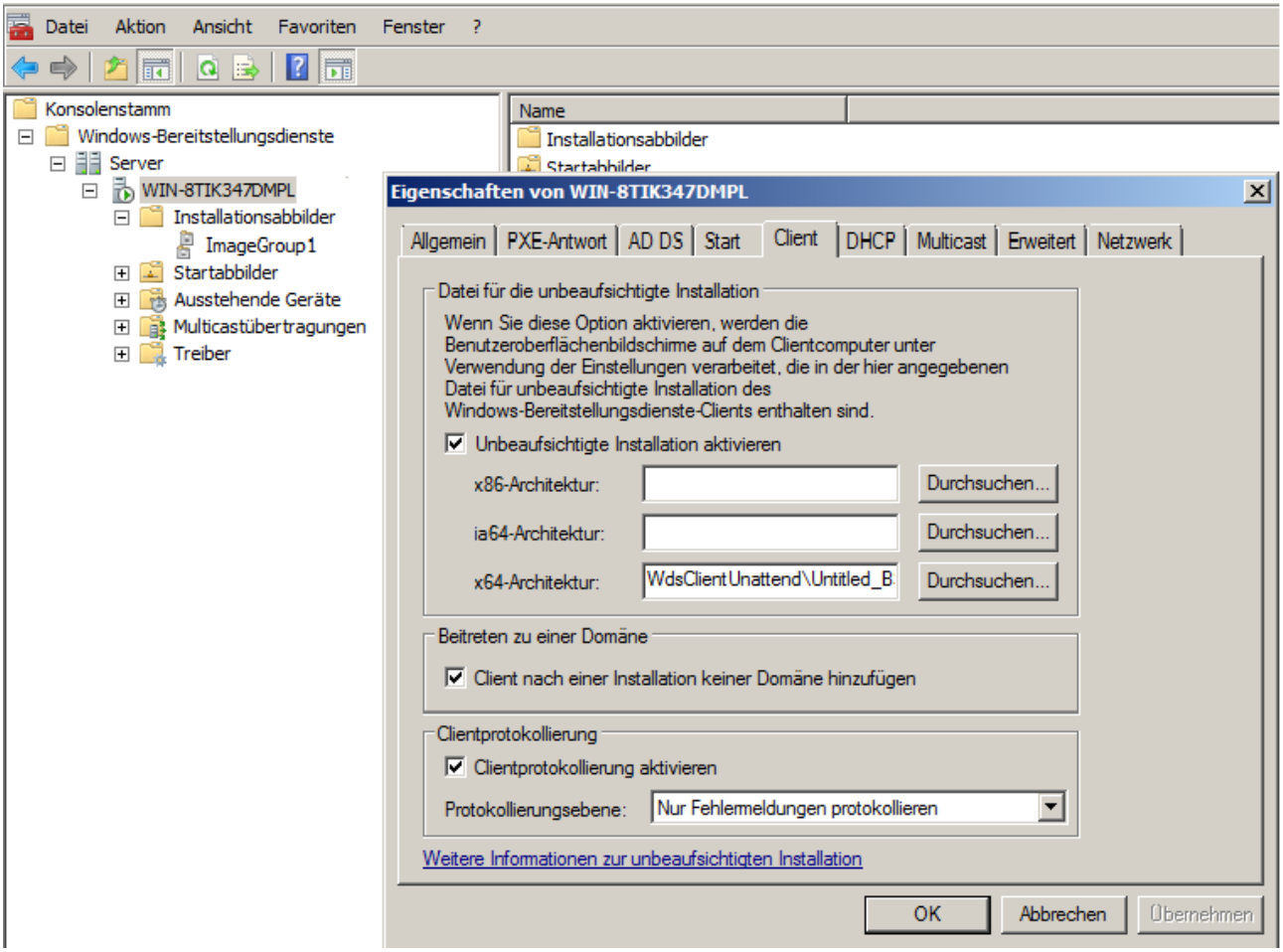


Abbildung 5.22: Einbindung einer Antwortdatei

Komponente	Einstellungen	Beschreibung
1 windowsPE amd64_Microsoft-Windows-International-Core-WinPE_neutral/ SetupUILanguage:	UILanguage: de-DE WillShowUI: OnError	Spracheinstellung für das Windows-Setup Anzeige des Setup Status
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/ Disk:	WillShowUI: OnError Action: AddList Item DiskID: 0 WillWipeDisk: true	Anzeige des Setup Status Eine physische Festplatte hinzufügen Hinzufügen der Disk-ID
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/ Disk/ Create Partitions/ Create Partitions	Action: AddList Item Extend: false Order: 1 Size: 100 Type: Primary	Erstellung einer erweiterten, primären und 100 MB großen Windows Systempartition auf der Disk “0“.
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/ Disk/ Create Partitions/ Create Partitions	Action: AddList Item Extend: true Order: 2 Size: Type: Primary	Erstellung einer zweiten, erweiterten, primären Windows Betriebssystempartition auf der Disk “0“. Wird keine Größe angegeben, wird die Partition mit dem verbliebenen Rest der Disk erstellt.
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/Disk/ ModifyPartition	Action: Modify Active: true Extend: false Format: NTFS Label: MBR Order: 1 PartitionID: 1	Konfiguration der Windows Systempartition, die aktiv und mit NTFS formatiert werden soll. Optional ist ein Name anzugeben, weiterhin die Reihenfolge der Partitionierung.
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/Disk/ ModifyPartition	Action: Modify Active: true Extend: false Format: NTFS Label: Windows_OS Letter: C Order: 2 PartitionID: 2	Konfiguration der Windows Betriebssystempartition, die aktiv und mit NTFS formatiert werden soll. Optional ist ein Benamung anzugeben. Optional ist ein Name anzugeben, weiterhin die Reihenfolge der Partitionierung.
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/UserData	Accept Eula: true Full Name: BSI_PC Organization: BSI	Zustimmung zu der Lizenzvereinbarung sowie der Beschreibung des Endbenutzers und der Organisation des APC.
1 windowsPE amd64_Microsoft-	Key: XXXXX-XXXXX-XXXXX-	Windows-Aktivierungsschlüssel

Komponente	Einstellungen	Beschreibung
Windows-Setup_neutral/ DiskConfiguration/UserData ProductKey	XXXXX-XXXXX WillShowUI: OnError	Anzeige des Setup Status Die „ProductKey“ Komponente wird dafür genutzt, dass der Windows Aktivierungs-schlüssel automatisch bei der Installation hinterlegt wird.
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/UserData/WindowsDeploymentService/ ImageSelection	WillShowUI: OnError	Anzeige des Setup Status Die „ImageSelection“ Komponente ist not-wendig für den Verweis auf das Imagefile. Dort, wo das Windows-Abbild innerhalb des Bereitstellungsdienst hinterlegt ist.
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/UserData/WindowsDeploymentService/ImageSelection/InstallImage	Filename: Win_7_Referenzsystem.wim ImageGroup: ImageGroup1 ImageName: Win_7	Hier wird der Dateiname des Windows-Abbilds (WIM) des erstellen Referenzsystems angegeben sowie die hinterlegte ImageGroupe und den bei der Erstellung des Windows-Abbilds definierten Namen.
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/UserData/WindowsDeploymentService/ImageSelection/InstallTo	DiskID: 0 PartitionID: 2	Das Windows-Abbild wird auf der Festplatte mit der ID = „0“ und der Partitions-ID = „2“ installiert. Die Systempartition samt Bootmanager wird vom Setup eigenständig angelegt.
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/UserData/WindowsDeploymentService/ImageSelection/Login	WillShowUI: OnError	Anzeige des Setup Status Die „Login“ Komponente ist notwendig für den Remote-Zugriff auf den Bereit-stellungsserver.
1 windowsPE amd64_Microsoft-Windows-Setup_neutral/ DiskConfiguration/UserData/WindowsDeploymentService/ImageSelection/LoginCredentials	Domain: BSI.local Passwort: Sicherheit Username: Administrator	Hier werden die Anmeldeinformationen hinterlegt, die für das erfolgreiche Einloggen auf dem Bereitstellungsdienst benötigt werden.

Tabelle 16: Konfigurationseinstellungen der Antwortdatei

5.4 Änderungen am Referenzsystem

Nachdem das Referenzsystem erstellt wurde, sollte dieses in einem dokumentierten Zustand und für alle Administratoren zugängig aufbewahrt werden. Sind Veränderungen an dem Referenzsystem vorzunehmen, z. B. durch Installationen von zusätzlichen Treibern, Updates oder Softwarepaketen, ist wie folgt vorzugehen:

1. Installation des Referenzsystems auf einem APC wie in Abschnitt 5.2 oder Abschnitt beschrieben.
2. Das installierte Referenzsystem als Administrator des APC mit folgendem Befehl in den Überwachungsmodus versetzen (s. h. Abschnitt): `sysprep.exe /audit`
3. Änderungen am APC durchführen (s. B. Treiberupdates, Hinzufügen von Software, Updates, etc.). Alle Komponenten auf Funktionsfähigkeit testen.
4. Mit dem Befehl `sysprep.exe /oobe` das angepasste Referenzsystems versiegeln und ggf. mit dem zusätzlichen Schalter `/generalize` noch entkernen, sofern dies notwendig sein sollte.
5. Neues Referenzsystem als Windows-Abbild erstellen.

5.5 Zentrale Aufrechterhaltung der Minimalisierung

Nach der Installation, Minimalisierung und Härtung des Betriebssystems sowie den benötigten Anwendungen folgt der tägliche Betrieb des APCs. Hierbei unterliegt der APC auch Veränderungen. Dies ist vor allem dann der Fall, wenn z. B.:

- der Anwender Berechtigungen zur Durchführung von Änderungen am System besitzt,
- Anwendungen ohne vorherige Sicherheitsbetrachtung nachinstalliert werden,
- der APC und die darauf installierten Anwendungen nicht gewartet werden.

Damit ein fortwährendes und gleichbleibend hohes Sicherheitsniveau in der Umgebung der Behörde oder Organisation bestehen bleibt, sind daher geeignete Maßnahmen zur Aufrechterhaltung der Minimalisierung umzusetzen.

Folgende technische oder organisatorische Maßnahmen können zur zentralen Aufrechterhaltung der Minimalisierung definiert werden:

- Auditierung
- Informationsauswertung
- Fernzugriffe

5.5.1 Auditierung

Die APCs werden in regelmäßigen Abständen lesend überprüft und der Ist-Zustand mit dem Soll-Zustand verglichen. Mit Hilfe eines Aktionsplans werden die Verstöße korrigiert oder nach einer Sicherheitsbetrachtung freigegeben. Weitere Informationen können im BSI-Leitfaden[102] „Informationssicherheitsrevision“ nachgelesen werden.

102 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v2_pdf.pdf?__blob=publicationFile

5.5.2 Informationsauswertung

Der APC stellt Informationen bereit, welche regelmäßig aktiv und bei Unregelmäßigkeiten sofort ausgewertet werden. Diese Informationen werden über sog. Logging-Funktionen bereitgestellt.

Unter Windows 7 werden die folgenden Werkzeuge hierfür bereitgestellt:

- Windows Eventing
- Windows Firewall Logging

Windows Eventing

Mit Windows Vista wurde eine neue Infrastruktur für Ereignisprotokollierung und Ablaufverfolgung namens Windows Eventing 6.0. eingeführt. Diese Funktion ist auch unter Windows 7 verfügbar. Welche Ereignisse wie protokolliert werden, wird über die Überwachung von Systemereignissen und den Einstellungen zum Ereignisprotokoll konfiguriert. Windows 7 verfügt über eine „Erweiterte Überwachungsrichtlinienkonfiguration“. Das Logging für die Windows-Firewall ist noch nicht in das Windows-Logging integriert. Für das zentrale Logging kann der APC so eingerichtet werden, dass die Log-Dateien an einen Abonnement-Manager-Server gesendet werden. Die Übertragung sollte verschlüsselt erfolgen, beispielsweise über HTTPS.

Die notwendigen Einstellungen können über das Gruppenrichtlinienobjekt „Überwachungsrichtlinie“ (siehe Abbildung 5.23) vorgenommen werden. Über Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → lokale Richtlinien → Überwachungsrichtlinie können die Parameter konfiguriert werden.

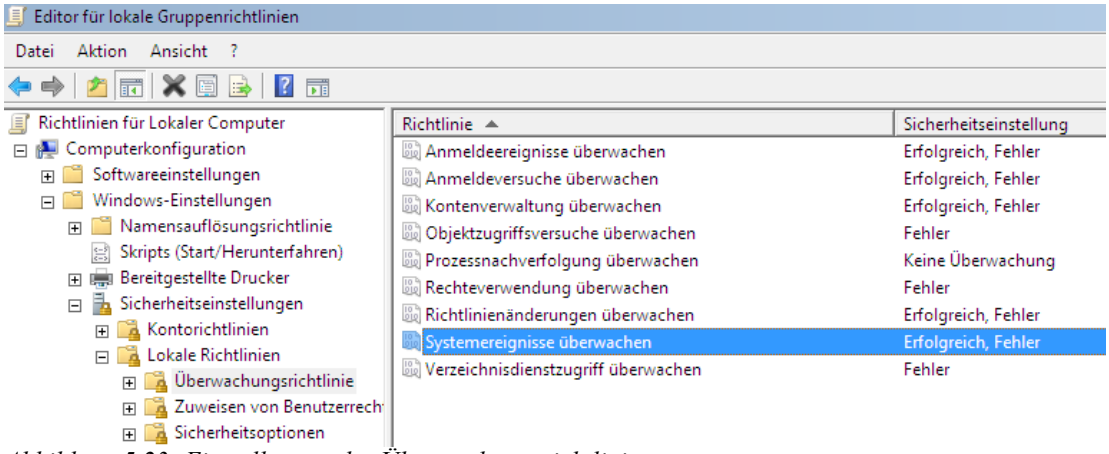


Abbildung 5.23: Einstellungen der Überwachungsrichtlinie

Folgende Parameter sind wie nachfolgend beschrieben entsprechend anzupassen:

Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → lokale Richtlinien → Überwachungsrichtlinie → Anmeldeereignisse überwachen

Default-Wert	Erfolgreich, Fehler
Neuer Wert	Erfolgreich, Fehler

Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → lokale Richtlinien → Überwachungsrichtlinie → Anmeldeversuche überwachen

Default-Wert	Erfolgreich, Fehler
Neuer Wert	Erfolgreich, Fehler

Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → lokale Richtlinien → Überwachungsrichtlinie → Kontenverwaltung überwachen

Default-Wert	Keine Überwachung
Neuer Wert	Erfolgreich, Fehler

Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → lokale Richtlinien → Überwachungsrichtlinie → Objektzugriffsversuche überwachen

Default-Wert	Keine Überwachung
Neuer Wert	Fehler

Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → lokale Richtlinien → Überwachungsrichtlinie → Prozessverfolgung überwachen

Default-Wert	Keine Überwachung
Neuer Wert	Keine Überwachung

Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → lokale Richtlinien → Überwachungsrichtlinie → Rechteverwendung überwachen

Default-Wert	Keine Überwachung
Neuer Wert	Fehler

Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → lokale Richtlinien → Überwachungsrichtlinie → Richtlinienveränderungen überwachen

Default-Wert	Keine Überwachung
Neuer Wert	Erfolgreich, Fehler

Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → lokale Richtlinien → Überwachungsrichtlinie → Systemereignisse überwachen

Default-Wert	Keine Überwachung
Neuer Wert	Erfolgreich, Fehler

Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → lokale Richtlinien → Überwachungsrichtlinie → Verzeichnisdienstzugriff überwachen

Default-Wert	Keine Überwachung
Neuer Wert	Fehler

Die erweiterte Überwachungsrichtlinienkonfiguration ermöglicht über die oben dargestellten Möglichkeiten hinausgehend weitere Konfigurationsmöglichkeiten.

Über Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → erweiterte Überwachungsrichtlinienkonfiguration können die Einstellungen vorgenommen werden. Abbildung 5.24 zeigt entsprechende Konfigurationsmöglichkeiten.

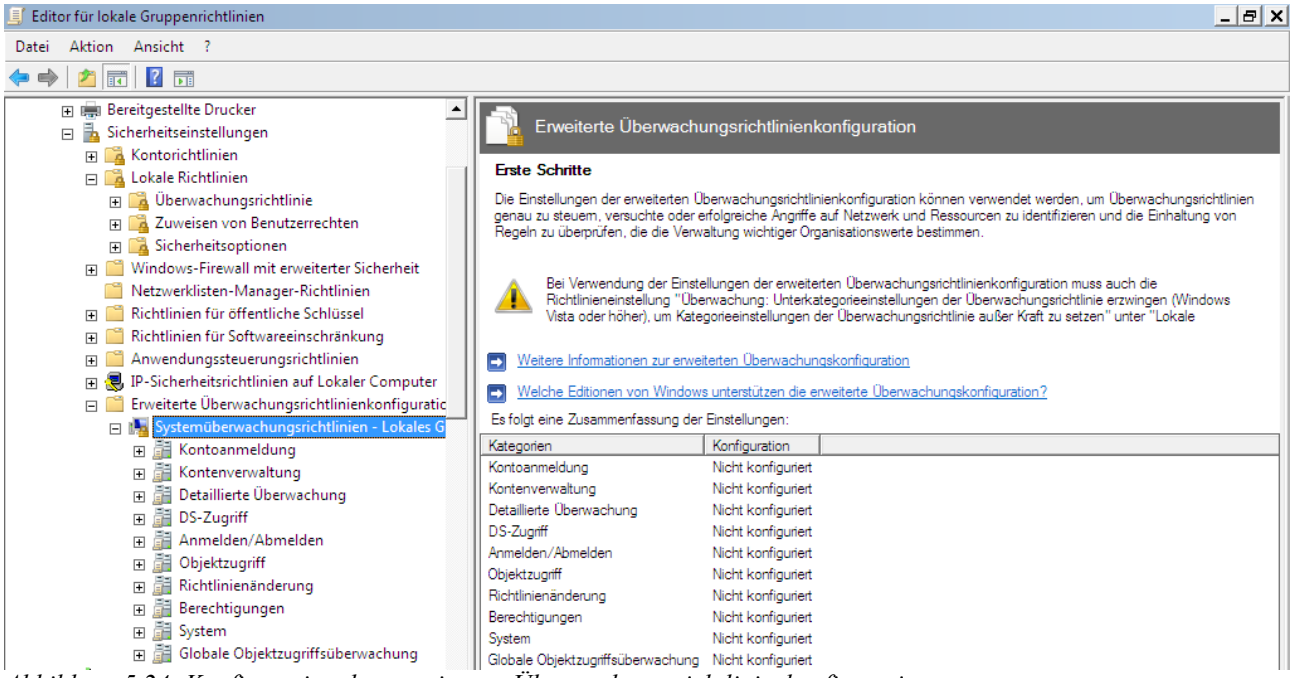


Abbildung 5.24: Konfiguration der erweiterten Überwachungsrichtlinienkonfiguration

Die folgende Abbildung 5.25 zeigt die Konfigurationsmöglichkeiten für die Kontenverwaltung unter Verwendung der erweiterten Überwachungsrichtlinienkonfiguration:

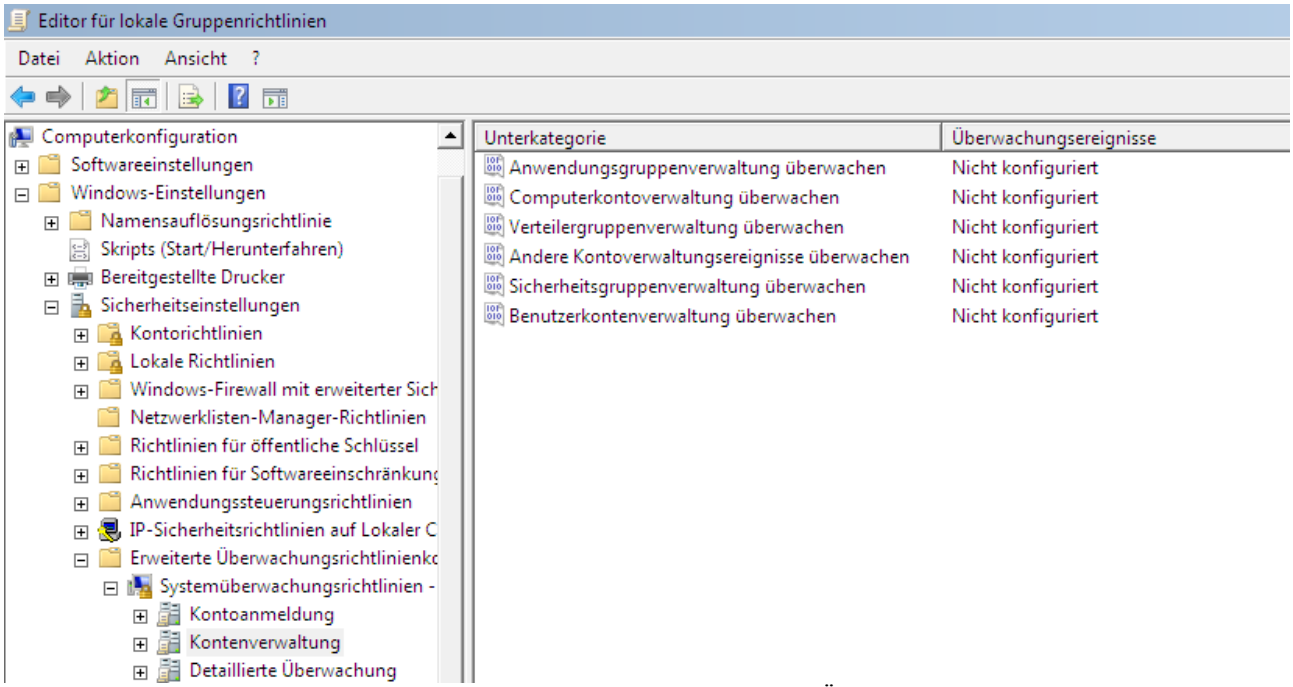


Abbildung 5.25: Einstellungen für die Kontenverwaltung in der erweiterten Überwachungsrichtlinienkonfiguration

Wichtiger Hinweis: Wenn die Einstellungen über die erweiterte Überwachungsrichtlinienkonfiguration vorgenommen werden, muss der Parameter
Computerkonfiguration → Windowseinstellungen → Sicherheitseinstellungen → Sicherheitsoptionen → Überwachung: Überschreiben der Einstellungen für Kategorie-Überwachungsrichtlinien durch die Einstellungen für Unterkategorie-Überwachungsrichtlilien (Windows Vista oder höher) erzwingen

aktiviert werden. Dies bedeutet, dass ab diesem Zeitpunkt die erweiterten Einstellungen Gültigkeit haben.

Des Weiteren sind die Parameter für das Ereignisprotokoll zu konfigurieren. Dies geschieht ebenfalls über Gruppenrichtlinienobjekte für Anwendungs-, Setup-, Sicherheits und Systemereignisse.

Folgende Werte sollten gesetzt werden:

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisweiterleitung | Serveradresse, Aktualisierungsintervall und Ausstellerzertifizierungsstelle eines Abonnement-Managers konfigurieren

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert, HTTPS verwenden

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | Anwendung | Alte Ereignisse beibehalten

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | Anwendung | Maximale Protokollgröße (kb)

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert, 30080 kb

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | Anwendung | Volles Protokoll automatisch sichern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | Setup | Alte Ereignisse beibehalten

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | Setup | Maximale Protokollgröße (kb)

Default-Wert	Nicht konfiguriert

Neuer Wert	Aktiviert, 30080 KB

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | Setup | Volles Protokoll automatisch sichern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | Sicherheit | Alte Ereignisse beibehalten

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert,

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | Sicherheit | Maximale Protokollgröße (kb)

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert, 100992 kb

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | Sicherheit | Volles Protokoll automatisch sichern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | System | Alte Ereignisse beibehalten

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | System | Maximale Protokollgröße (kb)

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert, 30080 kb

Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Ereignisprotokolldienst | System | Volles Protokoll automatisch sichern

Default-Wert	Nicht konfiguriert
Neuer Wert	Aktiviert

Logging mit der Windows Firewall

Windows 7 verfügt, wie auch seine Vorgängerversionen, über kein zentrales Logging der Firewall-Protokolle. Wenn sich der APC in einem Netzwerk befindet, kann die Anlage der Log-Dateien auf einen zentralen Server vorgenommen werden. Dabei ist zu beachten, dass das Firewall-Dienstkonto Schreibrechte auf dieses Verzeichnis erfordert. Mit der nachfolgenden Aktion kann die Protokollierung der Firewall definiert werden.

G

Start → Systemsteuerung → Windows Firewall → Erweitere Eigenschaften → Rechtsklick → Windows-Firewall mit erweiterter Sicherheit → Eigenschaften → Auswahl des Profils → unter Protokollierung → Anpassen → Verworfene Pakete protokollieren

Ereignisanzeige

Die Ereignisanzeige (engl. Event Viewer) ist ein erweitertes Werkzeug, das detaillierte Informationen über signifikante Ereignisse auf dem APC mitschreibt und anzeigt. Die Ereignisanzeige kann dann hilfreich sein, wenn Lösungen bei Problemen mit dem Betriebssystem oder den darauf betriebenen Anwendungen gesucht werden[103]. Um den Event-Viewer zu öffnen, ist die folgende Aktion auszuführen: Start → Systemsteuerung → Verwaltung → Ereignisanzeige

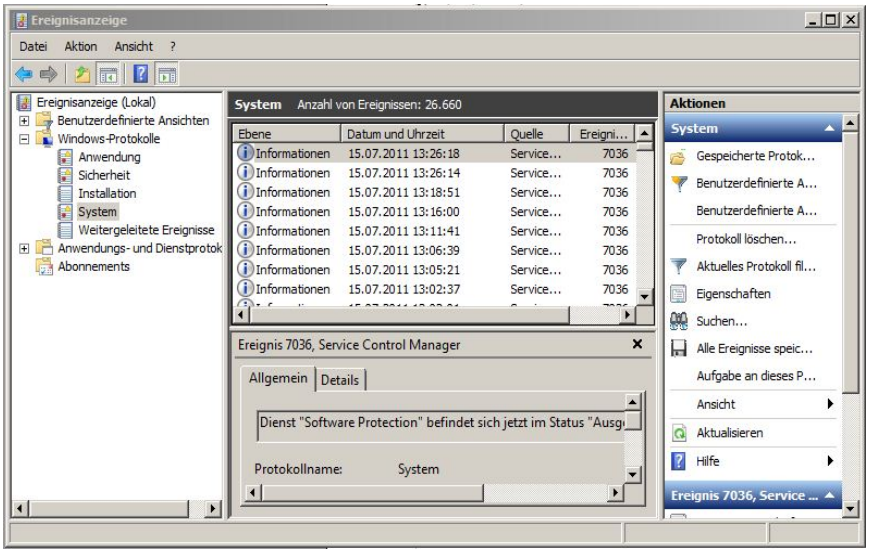


Abbildung 5.26: Ereignisanzeige

Die Windows-Logs beinhalten:

- Ereignisse von Anwendungen: Meldungen werden als Fehler, Warnung oder Information gekennzeichnet. Ein Fehler ist ein schwerwiegendes Problem, wie z. B. einem Datenverlust. Eine Warnung weist auf ein mögliches (zukünftiges) Problem hin. Eine Information gibt Meldung über eine erfolgreiche Abarbeitung einer Anwendung, eines Treibers oder eines Dienstes.
- Sicherheitsrelevante Ereignisse: Diese Nachrichtentypen werden auch als „Audits“ bezeichnet. Es werden erfolgreiche oder fehlgeschlagene Anmeldungen aufgezeichnet.
- Ereignisse bei Installationen: Systeme, die als Domänenkontroller spezifiziert wurden, tragen hier spezifische Meldungen ein.

103 http://windows.microsoft.com/en-US/windows-vista/Open-Event-Viewer

- Systemrelevante Ereignisse: System- und dienstspezifische Meldungen werden in die Kategorien Fehler, Warnung oder Information unterteilt.
- Weitergeleitete Ereignisse: In diesen Bereich werden Informationen von anderen APCs aus dem Netz geschrieben, sofern diese entsprechend konfiguriert sind.

5.5.2.1 Fernzugriffe

Die Konfiguration von APCs aus der Ferne, z. B. die Übermittlung von Konfigurationseinstellungen, kann sowohl mit Bordmitteln als auch durch zusätzliche Software erfolgen.

Remote-Registrierungsdienst

Über die entfernte Registrierungsdatenbank können bestimmte vordefinierte Schlüssel in der Registry geändert werden[104]. Diese Schlüssel sind:

- `HKEY_USERS`
- `HKEY_LOCAL_MACHINE`

Hierzu werden definierte APIs verwendet. Diese API spricht mit dem Remote-Registrierungsdienst. Hierzu muss dieser Dienst gestartet sein[105]. Dieser Dienst wurde in den Härtungsmaßnahmen unter Abschnitt 4.3.5.30 deaktiviert. Daher wird hier nur kurz auf eine Aktivierung eingegangen.

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst Remoteregistrierung → Eigenschaften → Klick auf die Auswahlbox rechts neben Starttyp → Automatisch

Start → Systemsteuerung → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → Rechtsklick auf den Dienst Remoteregistrierung → Starten

Zum Aufbau einer Verbindung zu einem APC, ist folgende Aktion[106] auszuführen:

Start → Eingabe von „Regedit“ in das Suchfeld → Der Registrierungseditor öffnet sich. → Datei → Mit Netzwerkregistrierung verbinden ... → Computer auswählen

104 http://support.microsoft.com/kb/256986
105 http://technet.microsoft.com/en-us/library/cc754820.aspx
106 http://technet.microsoft.com/de-de/library/cc785793(WS.10).aspx

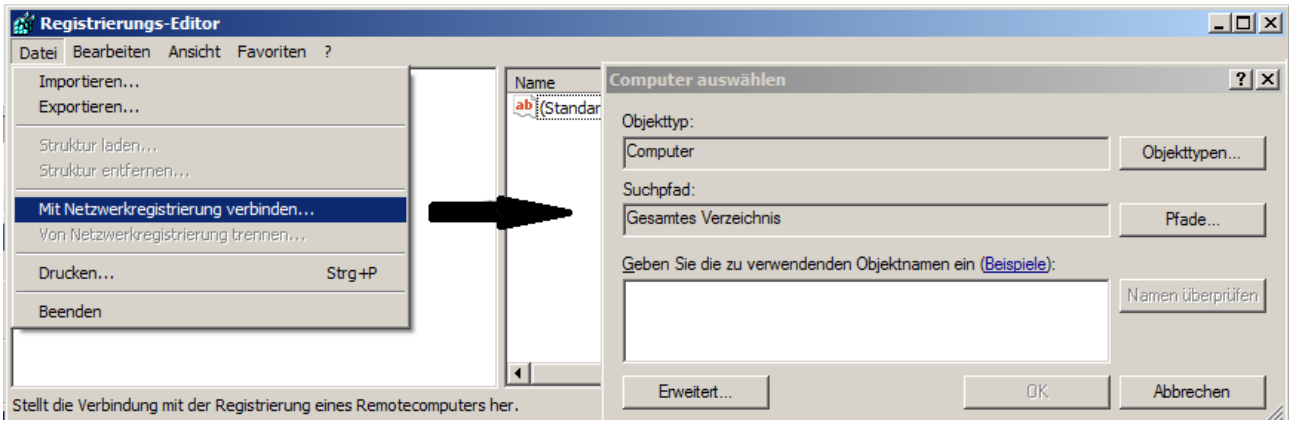


Abbildung 5.27: Zugriff auf die Remoteregistry

Scripting

Das Scripting, also das automatische Abarbeiten von einem oder mehreren Befehlen, kann unter Windows dazu verwendet werden, wiederkehrende Aufgaben in Dateien zusammenzufassen. Diese Dateien können kurze, aber auch große, über mehrere Seiten lange Befehlsverkettungen sein. Diese Dateien werden oftmals auch als Batch-Programme[107] bezeichnet. Jedoch können nicht nur Batch-Programme, sondern auch weitere Scriptsprachen (z. B. Perl, Jscript, VBscript) verwendet werden, wenn der entsprechende Interpreter installiert wurde.

Scripte können u. a. über die folgenden Befehlszeilenprogramme aufgerufen und/oder gesteuert werden:

- Eingabeaufforderung (`cmd.exe`)
- Windows Power Shell[108]
- WMI mit WMIC

Um eine Windows-basierte Umgebung mittels Skripten zu steuern und zu sichern, ist ein sicherer Umgang mit den entsprechenden Werkzeugen erforderlich. Erste Erfahrungen zum Thema Scripting können unter folgenden Links gesammelt werden:

- http://technet.microsoft.com/en-us/scriptcenter/bb410849
- http://technet.microsoft.com/en-us/library/bb902776.aspx

Active Directory

Das Active Directory (AD) ist der Verzeichnisdienst von Microsoft und stellt eine eine zweckgebundene Konfigurationsdatenbank[109] dar. Dieser Verzeichnisdienst ersetzt nicht die auf den APCs existierende Registrierungsdatenbank. Ist ein APC Mitglied in einer Domäne, so bekommt dieser aus der Konfigurationsdatenbank alle definierten Vorgaben übermittelt.

Diese Vorgaben werden als Domänenrichtlinien bezeichnet. Mittels Domänenrichtlinien lassen sich mehrere APCs, die einer Domäne angehören, gleich konfigurieren. Der Domänenkontroller ist zur

107 http://technet.microsoft.com/en-us/library/bb490869.aspx
108 http://technet.microsoft.com/de-de/library/bb978526.aspx
109 http://msdn.microsoft.com/en-us/library/aa746492(v=vs.85).aspx

Bereitstellung eines Active-Directory entsprechend zu konfigurieren[110]. Ein Domänenkontroller stellt hierzu mehrere Werkzeuge und Dienste bereit[111]. Ebenfalls ist sicher zu stellen, dass sich die zu härtenden Windows 7 APCs in einer entsprechende Organisationseinheit[112] der AD befinden. Dies ist notwendig, damit die GPO-Richtlinien nicht auch auf anderen Rechnern dieser Domäne (z. B. auf den Domänenkontroller selbst) angewendet werden.

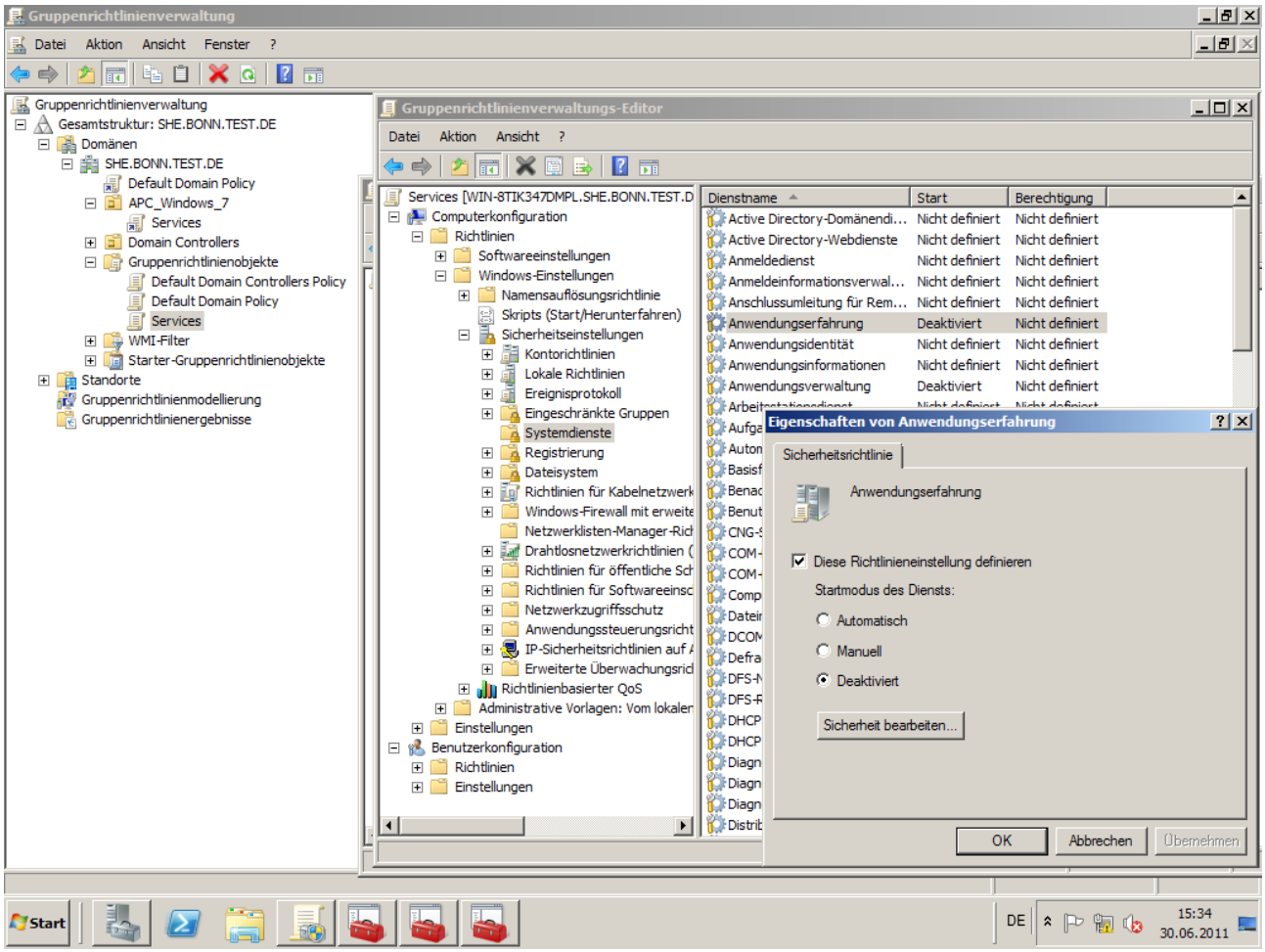


Abbildung 5.28: Zentrale Gruppenrichtlinienverwaltungs-Editor unter Windows 2008 R2

110 http://technet.microsoft.com/de-de/library/cc755258(WS.10).aspx
111 http://www.microsoft.com/windowsserver2008/en/us/ad-main.aspx
112 http://technet.microsoft.com/en-us/library/cc753063.aspx

6 Schlussbemerkung

Diese Leitlinie gibt Hinweise und Empfehlungen zur Absicherung von Arbeitsplatz-PCs mit Windows 7. Die einzelnen Schritte Installation, Minimierung, Konfiguration und Wartung lassen sich nicht generalisieren und bedürfen in der Regel Anpassungen an unternehmens- bzw. behördenspezifische Gegebenheiten. Beispiele hierfür sind die Verwendung von Remotedesktop zur Administration und der Einsatz einer Softwareverteilung zum Ausrollen von Images und Updates.

Des Weiteren geht diese Leitlinie nur auf die Absicherung des Betriebssystems an sich ein. Weitere Anwendungen wie Web-Browser, E-Mail-Clients, PDF-Betrachter oder Office-Programme müssen separat abgesichert werden. Beispiele hierfür sind das Deaktivieren der Ausführung aktiver Inhalte in E-Mails oder in PDF-Betrachtern.

Hinweise zur Absicherung von Anwendungen finden sich beispielsweise in den BSI-Studien *Sichere Nutzung von* Web-*Angeboten* [ISi-Web-Client] und *Sichere Nutzung von* E-Mail [ISi-Mail-Client].

Anmerkungen und Anregungen zur Pflege und Verbesserung dieses Dokumentes können Sie per E-Mail an isi-redaktion@bsi.bund.de richten.

7 Literaturverzeichnis

[ISi-Client] Bundesamt für Sicherheit in der Informationstechnik, Absicherung eines Clients, 2010

[ISi-LANA] Bundesamt für Sicherheit in der Informationstechnik, Sichere Anbindung lokaler Netze an das Internet, 2007

[ISi-Mail-Client] Bundesamt für Sicherheit in der Informationstechnik, Sichere Nutzung von E-Mail, 2009

[ISi-Web-Client] Bundesamt für Sicherheit in der Informationstechnik, Sichere Nutzung von Web-Angeboten, 2009