

# Neuerungen in Windows 7

Christian Zahler

## 4 Windows 7-Verwaltung

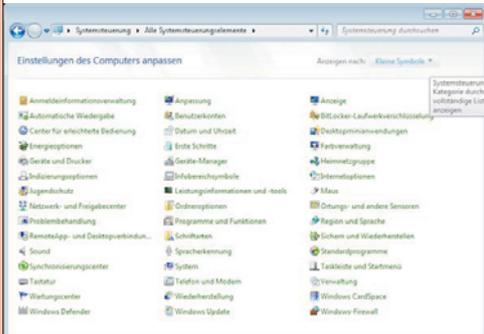
### 4.1 Systemsteuerung (engl. Control Panel)

Nach wie vor können gängige Administrationstätigkeiten über die Systemsteuerung durchgeführt werden.

Die Systemsteuerung gruppiert die Symbole in Aufgabenbereiche (die bis Windows Vista vorhandene "klassische" Ansicht gibt es nicht mehr).

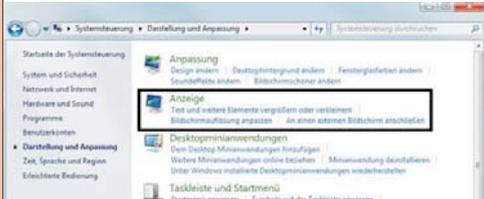


Die Ansicht der Systemsteuerung kann auch so umkonfiguriert werden, dass für jede \*.cp1-Datei (Abkürzung für „Control Panel“) ein großes oder kleines Symbol angezeigt wird:

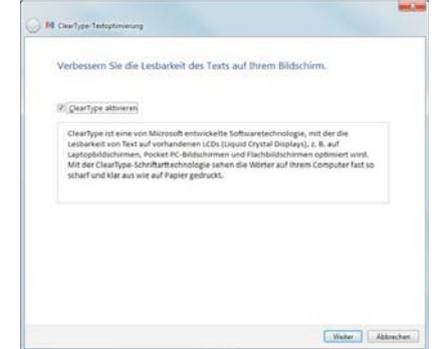
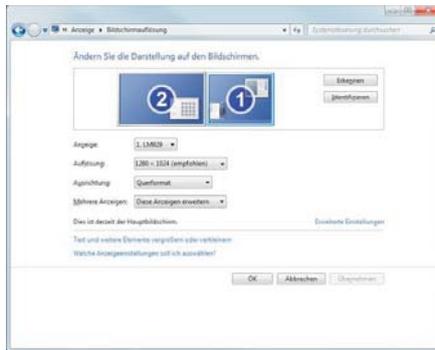


### 4.2 Anpassen der Bildschirmeinstellungen

Im Systemsteuerungspunkt „Darstellung und Anpassung“ können Sie unter „Anzeige“ die Bildschirmdarstellung, die Auflösung und weitere Parameter anpassen.



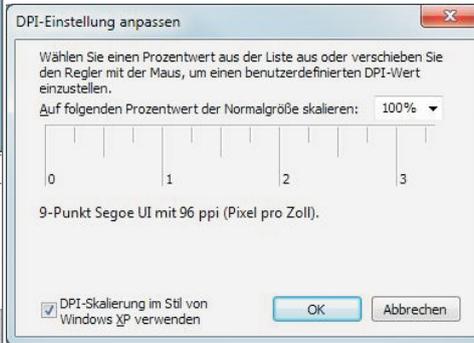
Besonderer Wert wurde auf die Lesbarkeit gelegt. So ist es nun auf einfache Weise möglich, die Größe der Systemschriftarten festzulegen.



Werden beispielsweise zwei Bildschirme verwendet, so kann die Anordnung der Bildschirme ebenfalls konfiguriert werden:

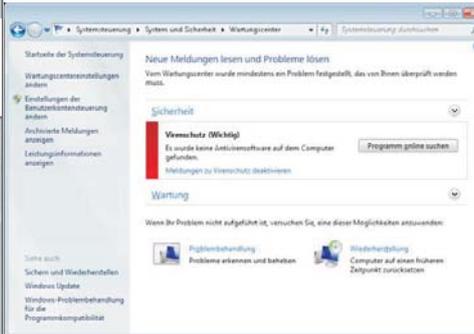
Die Aktivierung von „ClearType“ ist bei Verwendung tragbarer PCs empfehlenswert.

Schließlich kann auch eine benutzerdefinierte Textgröße festgelegt werden:



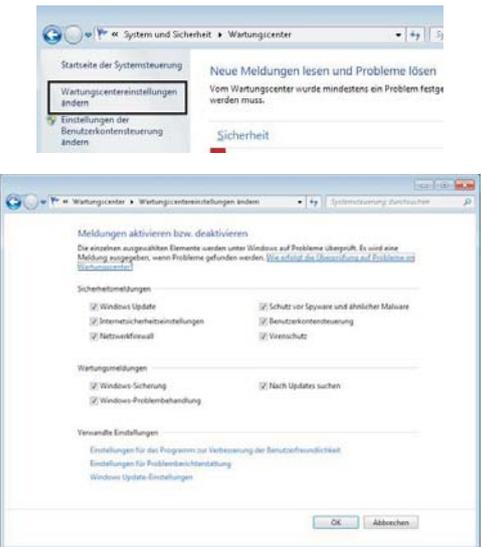
### 4.3 Wartungszentrum (engl. Action Center)

Im neuen Wartungszentrum sind Sicherheitseinstellungen und allgemeine Problembehandlungsaufgaben zusammengefasst.



### 4.3.1 Konfigurieren von Benachrichtigungen und Meldungen

Im Wartungszentrum gibt es die Möglichkeit, das Ausmaß von System-Benachrichtigungen zu konfigurieren:



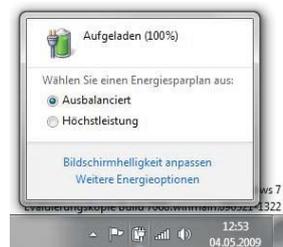
### 4.4 Energieverwaltung

Mit Windows 7 ist auch die verstärkte Betonung von Umweltaspekten eingeführt worden, die unter dem Schlagwort **Green IT** bekannt sind.

Mit der verbesserten Unterstützung für Remoteaktivierung über LAN (Wake on LAN, WoL) kann bei Windows 7-Computern der Stromverbrauch gesenkt werden, indem sie in den Standbymodus wechseln und länger in diesem Modus bleiben. Durch eine differenzierte Steuerung der Reaktivierungspakete bleibt der Computer länger im Standbymodus. Durch Verlagern der Protokollverarbeitung auf den Netzwerkadapter kann ein Computer im Standbymodus weiterhin für Netzwerkverwaltungstools erreichbar bleiben, ohne reaktiviert zu werden. Windows 7 unterstützt außerdem Remoteaktivierung über Drahtlos-LAN (Wake on Wireless LAN, WoWLAN), wodurch Standby-szenarios auf drahtlose Clientcomputer erweitert werden.

In Windows 7 kann der Energieverbrauch darüber hinaus reduziert werden, indem die Stromzufuhr für den Netzwerkadapter deaktiviert wird, wenn das Kabel getrennt wird. Wenn der Benutzer ein Kabel anschließt, wird die Stromversorgung automatisch wiederhergestellt.

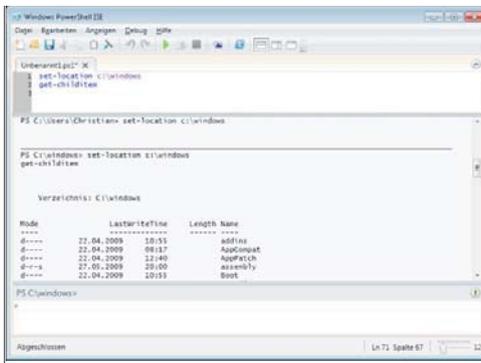
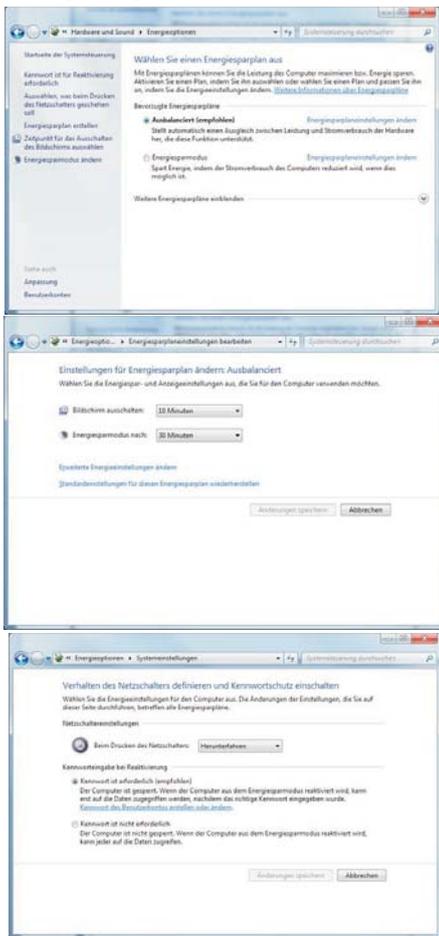
So wird zum Beispiel beim schnellen Wechsel des Energiesparmodus über das Icon im Benachrichtigungsbereich jetzt immer der Energiesparplan Höchstleistung mit angezeigt. Standardmäßig wird Windows 7 im Modus Ausbalanciert betrieben, was einen guten Kompromiss zwischen Akkulaufzeit und Performance darstellt. Immer wenn zum Beispiel ein Vortrag gehalten wird, schaltet man auf Höchstleistung. Dieses Umschalten ist jetzt viel einfacher.



http://www.microsoft.com/windows/windows-7/

CLUBSYSTEM.NET

In der Systemsteuerung kann die Energieverwaltung konfiguriert werden:

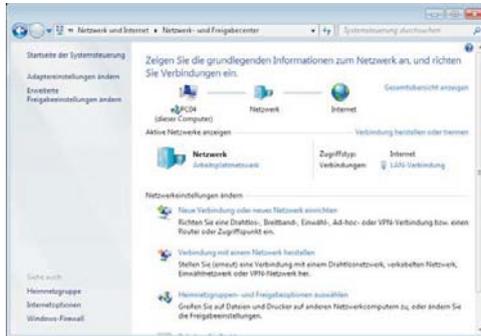


### 5 Windows 7 im Netzwerk

#### 5.1 Netzwerkstandort und Firewallprofile

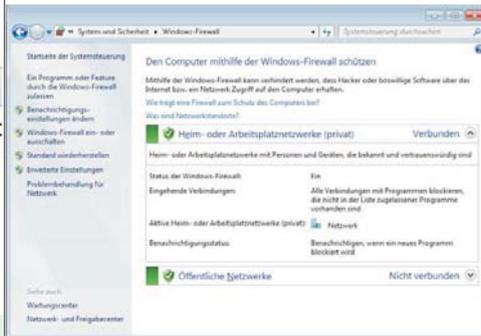
Für den Netzwerkbetrieb ist es nötig, dass alle PCs Netzwerkkarten aufweisen.

Die Konfiguration der wichtigsten Netzwerkeinstellungen ist am einfachsten über das Netzwerk- und Freigabecenter möglich.



Die Netzwerkschnittstellen müssen seit Windows Vista einem Netzwerkstandort zugewiesen werden. Die Auswahl des Netzwerkstandorts legt gleichzeitig Firewallprofile fest. Die "strengste", aber auch sicherste Einstellung ist "Öffentliches Netzwerk".

Neu in Windows 7 und Windows Server 2008 R2 ist die Möglichkeit, gleichzeitig mehrere Firewallprofile aktiv zu haben.

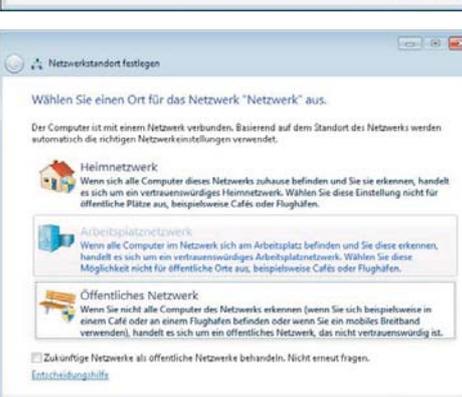
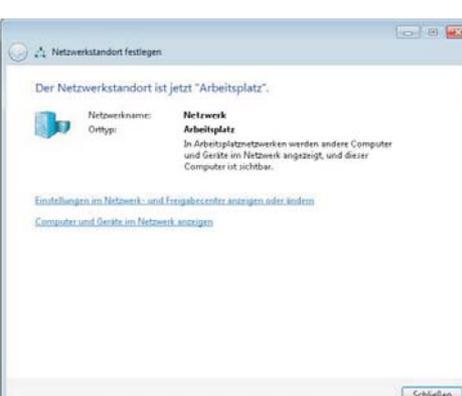


Die Windows Firewall-Einstellungen werden von dem Profil bestimmt, das Sie verwenden. In früheren Windows-Versionen kann jeweils nur ein Firewallprofil aktiv sein. Wenn daher mehrere Netzwerkkarten mit unterschiedlichen Netzwerktypen verbunden sind, ist trotzdem nur ein aktives Profil verfügbar: das Profil mit dem am stärksten einschränkenden Regeln. In Windows Server 2008 R2 und Windows 7 wendet jeder Netzwerkkarten das Firewallprofil an, das am besten für den Netzwerktyp geeignet ist, mit dem eine Verbindung besteht: Privat, öffentlich oder Domäne. Wenn Sie also in einem Café mit einem Drahtlos-Hotspot über VPN eine Verbindung mit dem Domänennetzwerk des Unternehmens herstellen, bedeutet dies, dass mit dem Profil Öffentlich der Netzwerkverkehr, der nicht durch den Tunnel gesendet wird, weiter geschützt wird, wäh-

rend mit dem Profil Domäne der Netzwerkverkehr geschützt wird, der den Tunnel passiert. So wird auch das Problem von nicht mit dem Netzwerk verbundenen Netzwerkkarten berücksichtigt. In Windows 7 und Windows Server 2008 R2 wird diesem nicht identifizierten Netzwerk das Profil Öffentlich zugewiesen, und die anderen Netzwerkkarten auf dem Computer verwenden weiter das für das Netzwerk, mit dem eine Verbindung besteht, am besten geeignete Profil.

#### 5.1.1 Arbeitsplatznetzwerk

Der Netzwerkstandort "Arbeitsplatznetzwerk" legt Firewallregeln fest, die für einen üblichen Büro-Arbeitsplatz sinnvoll sind.



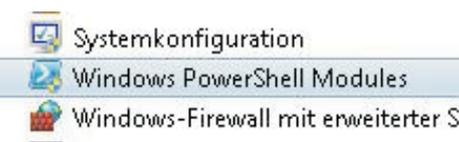
#### 5.2 Heimnetzwerk und Heimnetzgruppe (Homegroup)

Dieses unter Windows 7 neue Feature soll die Konfiguration von Netzwerken im Privatbereich erheblich vereinfachen. Dabei sollen Bilder, Musik und Geräte wie Drucker über das Netzwerk zur gemeinsamen Nutzung freigegeben werden. Einzig die Kenntnis eines Kennwortes reicht zur Erstellung und Teilnahme aus. Das Arbeitsgruppen-Konzept wird hier nicht benötigt. Kommen Freunde zu Besuch, können sie sich schnell und unkompliziert ins Heimnetz einklinken und daran teilnehmen.

### 4.5 PowerShell 2.0

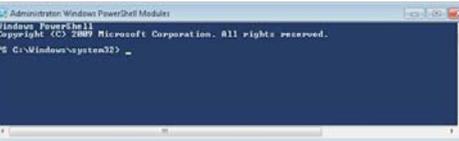
Integrierter Bestandteil von Windows 7 und Windows Server 2008 R2 ist die neue Version der PowerShell.

Die PowerShell kann im Verwaltungsmenü aufgerufen werden und benötigt erhöhte Rechte (User Account Control).



Beim ersten Start wird versucht, Module zu importieren. Falls eine Fehlermeldung auftritt, so müssen Sie möglicherweise zuerst die Ausführung unsignierter Powershell-Skripts erlauben:

**Set-ExecutionPolicy Unrestricted**  
Ab dann können alle PowerShell-Cmdlets und -Skripts problemlos ausgeführt werden.



Neu in PowerShell 2.0 ist die Remoting-Funktionalität. Das bedeutet, dass Powershell-Befehle lokal eingegeben werden, aber auf einem anderen PC (oder mehreren anderen PCs) ausgeführt werden können. Dieses neue Feature beruht auf WinRM (Windows Remote Management).

PowerShell-Skripte können nun einfacher im PowerShell ISE (Integrated Scripting Environment) getestet und erstellt werden.

CLUBSYSTEM.NET

http://www.microsoft.com/windows/windows-7/

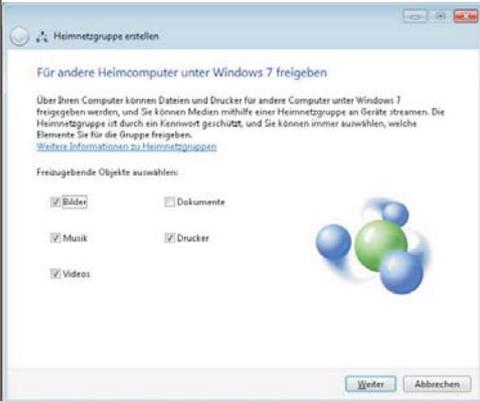
Voraussetzungen:

- Alle Rechner, die Mitglieder einer Homegroup sind, müssen mit Windows 7 betrieben werden. Windows XP und Windows Vista können die Heimnetzgruppe nicht erkennen bzw. ausführen.
- IPv6 muss aktiviert sein.

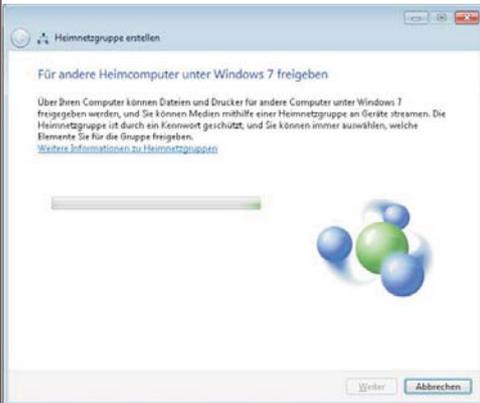
Technisch wird für die Heimnetzgruppe das Protokoll IPv6 in Kombination mit der Namensauflösungstechnologie **PNRP** (Peer Name Resolution Protocol) verwendet. Diese Technologien werden im Skripten "Windows Server 2008 – Netzwerkinfrastruktur" detailliert behandelt.

5.2.1 Erstellen einer Heimnetzgruppe

Dazu ist ein Rechner erforderlich, auf dem mindestens Windows 7 Home Premium installiert ist. Zunächst muss als Netzwerkstandort "Heimnetz" ausgewählt werden:



An dieser Stelle können Sie alle vier vorhandenen **Standardbibliotheken** freigeben, zusätzlich ist die gemeinsame Verwendung von Druckern vorgesehen.



Sollte in der Systemsteuerung bereits eine Heimnetzgruppe aktiv sein und man bekommt nur die Option "Heimnetzgruppeneinstellung ändern", kann dies folgende Ursache haben: Wurde bei einer Installation ein Netzwerk-

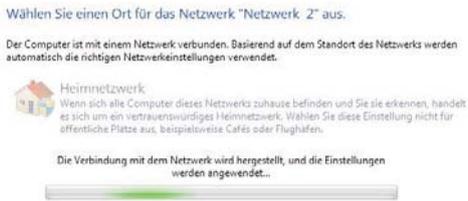


dapter und eine aktive Netzwerkverbindung festgestellt, so teilt Windows schon bei der ersten Anmeldung ein Kennwort für die Heimnetzgruppe mit.

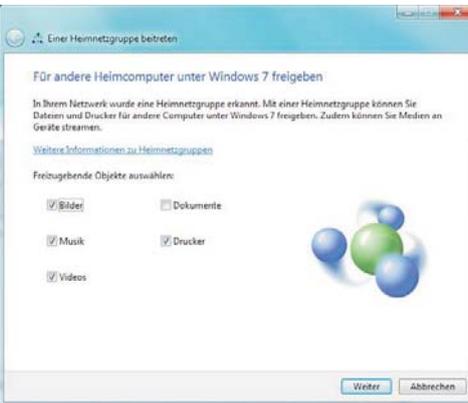
5.2.2 Beitritt zu einer bestehenden Heimnetzgruppe

Um sinnvoll mit Heimnetzgruppen arbeiten zu können, müssen Sie nun mit allen weiteren Computern der eben erstellten Heimnetzgruppe beitreten.

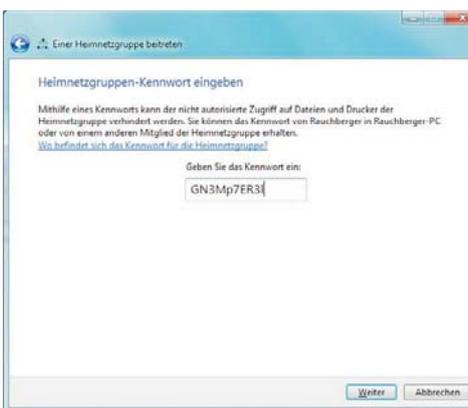
Dazu wählen Sie wieder als Netzwerkstandort "Heimnetz".



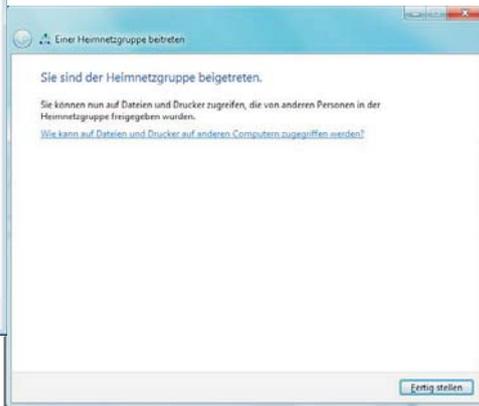
Es wird automatisch erkannt, dass im lokalen IP-Netzwerk eine Heimnetzgruppe eingerichtet wurde.



Geben Sie im nächsten Schritt das Kennwort für die Heimnetzgruppe an. Dieses Kennwort



hat der Benutzer erhalten, der die Heimnetzgruppe angelegt hat.



5.2.3 Arbeiten in der Heimnetzgruppe

Wenn Sie im Windows-Explorer auf das Symbol „Heimnetzgruppe“ klicken, so sehen Sie alle beigetretenen Benutzer sowie in Klammern den Computernamen, auf dem diese Benutzer arbeiten.



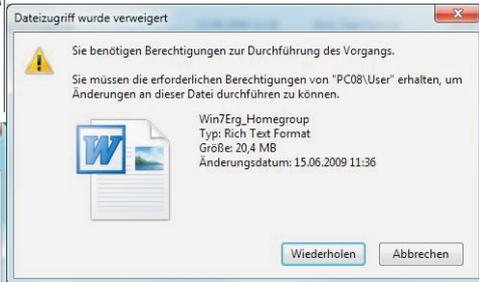
Erweitert man einen User, so sieht man dieselbe Bibliotheksstruktur wie auf dem lokalen Rechner.



Die darin vorhandenen Dateien können nun gemeinsam genutzt werden.

5.2.4 Berechtigungen

Löschvorgänge können von anderen Heimnetzbenutzern nur durchgeführt werden, wenn vom Urheber als Berechtigungsstufe „Lesen/Schreiben“ vergeben wurde. Sonst erscheint folgende Fehlermeldung:



5.2.5 Medienstreaming aktivieren

Standardmäßig ist Medienstreaming deaktiviert. Sie können unter Systemsteuerung – Netzwerk und Internet – Heimnetzgruppe das Medienstreaming aktivieren:

http://www.microsoft.com/windows/windows-7/

CLUBSYSTEM.NET

Heimnetzgruppen-Einstellungen ändern

Dieser Computer gehört zu einer Heimnetzgruppe.

Bibliotheken und Drucker freigeben

Bilder  Musik  Videos

Dokumente  Drucker

Wie können zusätzliche Bibliotheken freigeben werden? Wie werden Dateien und Ordner ausgeschlossen?

Medien für Geräte freigeben

Eigene Bilder, Musik und Videos an alle Geräte im eigenen Heimnetzwerk streamen

Medienstreamingoptionen auswählen

Hinweis: Freigegebene Medien sind nicht sicher. Alle Personen, die eine Verbindung mit Ihrem Netzwerk besitzen, können Ihre freigegebenen Medien empfangen.

Weitere Heimnetzgruppen-Aktionen

Kenntwort für die Heimnetzgruppe anzeigen oder drucken

Kenntwort ändern...

Heimnetzgruppe verlassen...

Erweiterte Freigabeinstellungen ändern...

Heimnetzgruppen-Problembearbeitung starten

### 5.2.6 Heimnetzgruppenprobleme lösen

**Beispiel 1:** In der Systemsteuerung erscheint folgende Meldung:

Auf diesem Computer kann keine Verbindung mit einer Heimnetzgruppe hergestellt werden.

Die Heimnetzgruppe ist noch nicht bereit. Wiederholen Sie den Vorgang in einigen Minuten. Wenn diese Meldung weiterhin angezeigt wird, klicken Sie auf den Link, um die Heimnetzgruppen-Problembearbeitung zu starten.

Heimnetzgruppen-Problembearbeitung starten

Mit einer Heimnetzgruppe können Sie Dateien und Drucker für andere Computer unter Windows 7 freigeben. Zudem können Sie Medien an Geräte streamen. Die Heimnetzgruppe ist durch ein Kennwort geschützt, und Sie können immer auswählen, welche Elemente Sie für die Gruppe freigeben.

Mögliche Ursache für diese Fehlermeldung ist die Umkonfiguration des Netzwerkprofils (auf „Domäne“ oder „Öffentlich“). Mit dem Problembearbeitungs-Assistenten kann dieses Problem jedoch leicht behoben werden.

**Beispiel 2:** Beim Klicken auf „Heimnetzgruppe“ kommt folgende Meldung:

Derzeit sind keine anderen Heimnetzgruppen-Computer verfügbar.

Stellen Sie Folgendes sicher:

- Die anderen Heimnetzgruppen-Computer sind eingeschaltet und mit dem Netzwerk verbunden.
- Die Netzwerkadresse dieses Computers und der anderen Heimnetzgruppen-Computer ist auf 'Privat' festgelegt.
- Die anderen Heimnetzgruppen-Computer verfügen über das aktuelle Heimnetzgruppen-Kennwort.
- Andere Personen in Ihrer Heimnetzgruppe geben Bibliotheken für die Heimnetzgruppe frei.

View homegroup settings

Start the HomeGroup troubleshooter

Mit dem Fehlerbehandlungs-Assistenten können häufige Probleme erkannt und behoben werden:

Probleme werden ermittelt.

Starting HomeGroup diagnostics...

Computerprobleme behandeln und Computerproblemen vorbeugen

Heimnetzgruppe

Zugriff Computer oder freigegebene Dateien in einer Heimnetzgruppe an.

Erweitert

Herausgeber: Microsoft Corporation

Datenschutzbestimmungen online lesen

Heimnetzgruppe

Allow HomeGroup to communicate through Windows Firewall

Windows Firewall is preventing HomeGroup from communicating. Windows can automatically enable communication through the firewall, which might resolve the problem.

Diese Korrektur anwenden

Diese Korrektur überspringen

Problembehandlung fortsetzen, ohne diese Korrektur anzuwenden.

Abbrechen

Problembehandlung abgeschlossen

Von der Problembehandlung konnten nicht alle gefundenen Probleme behoben werden. Ausführlichere Informationen finden Sie weiter unten.

Gefundene Probleme

Windows Firewall is incorrectly configured Nicht behoben

The HomeGroup permissions are incorrect Nicht behoben

Zusätzliche Optionen durchsuchen

Problembehandlung schließen

Ausführlichere Informationen anzeigen

Schließen

### 5.2.7 Windows-Firewalleinstellungen für Heimnetzgruppen

Eine häufige Ursache für Probleme im Zusammenhang mit Heimnetzgruppen sind falsche Einstellungen für die Windows-Firewall.

**Hinweis:** Ein Domänen-Mitgliedscomputer kann auch gleichzeitig Mitglied einer Heimnetzgruppe sein.

Systemsteuerung > System und Sicherheit > Windows Firewall

Den Computer mithilfe der Windows-Firewall schützen

Mithilfe der Windows-Firewall kann verhindert werden, dass Hacker oder bösartige Software über das Internet Ihren PC über ein Netzwerk zuhause auf dem Computer infizieren.

Sie legen eine Firewall zum Schutz des Computers fest.

Windows-Firewall

Diagnose-Netzwerke Nicht verbunden

Heim- oder Arbeitsplatznetzwerke (privat) Verbunden

Heim- oder Arbeitsplatznetzwerke mit Personen und Geräten, die bekannt und vertrauenswürdig sind

Status der Windows-Firewall Ein

Alle Verbindungen mit Programmen blockieren, die nicht in der Liste zugelassener Programme vorhanden sind

Alleinstufige Firewall

Netzwerk 4

Netzwerk 4

Alle Verbindungen mit Programmen blockieren, die nicht in der Liste zugelassener Programme vorhanden sind

Einzelstufige Firewall

Öffentliche Netzwerke Nicht verbunden

Öffentliche Netzwerke

Alle Verbindungen mit Programmen blockieren, die nicht in der Liste zugelassener Programme vorhanden sind

Achten Sie besonders auf die Regeln, die das **PNRP-Protokoll** betreffen: So müssen die Ports TCP 3587 und UDP 3540 in beiden Richtungen freigeschaltet sein. Sie finden die vordefinierten Regeln unter der Rubrik „Heimnetzgruppe“.

### 5.3 Standardmäßige Benutzerverwaltung (Windows 7 Home-Methode)

Standardmäßig erfolgt die Benutzerverwaltung über die Systemsteuerung, Punkt „Benutzerkonten“:

Systemsteuerung > Benutzerkonten

Benutzerkonten

Eigene Kennwörter ändern

Kontotyp ändern

Windows CardSpace

Anmeldeinformationsverwaltung

Windows-Anmeldeinformationen verwalten

Mail

Systemsteuerung > Benutzerkonten > Benutzerkonten

Änderungen am eigenen Konto durchführen

Eigenes Kennwort ändern

Eigenes Kennwort entfernen

Eigenes Bild ändern

Eigenen Kontonamen ändern

Eigenen Kontotyp ändern

Andere Konten verwalten

Einstellungen der Benutzerkontensteuerung ändern

Christian Administrator Kennwortgeschützt

Für jedes hier sichtbare Konto lassen sich Änderungen durchführen:

Änderungen am eigenen Konto durchführen

Eigenes Kennwort ändern

Eigenes Kennwort entfernen

Eigenes Bild ändern

Eigenen Kontonamen ändern

Eigenen Kontotyp ändern

Anderes Konto verwalten

Einstellungen der Benutzerkontensteuerung ändern

Christian Administrator Kennwortgeschützt

Eine neue Möglichkeit unter Windows 7 steht unter **„Eigene Anmeldeinformationen verwalten“** zur Verfügung. Damit lassen sich die Anmeldeinformationen in einem **„Windows-Tresor“** speichern:

Systemsteuerung > Anmeldeinformationsverwaltung

Anmeldeinformationen für automatisches Anmelden speichern

Mit der Anmeldeinformationsverwaltung können Sie Anmeldeinformationen von Benutzernamen und Kennwörtern in Tresoren speichern, um sich mühelos bei Computern oder Web Sites anzumelden.

Windows-Tresor

Standardspeicherort für Tresor

Tresor wiederherstellen

Windows-Anmeldeinformationen

Windows-Anmeldeinformationen hinzufügen

Es sind keine Windows-Anmeldeinformationen vorhanden.

Siehe auch

Benutzerkonten

Online-ID's verknüpfen

Zertifikatbasierte Anmeldeinformationen

Zertifikatbasierte Anmeldeinformationen hinzufügen

Auch zertifikatbasierte Anmeldeinformationen lassen sich solcherart speichern:

Systemsteuerung > Anmelde... > Zertifikatbasierte Anmeldeinformationen hinzufügen...

Geben Sie die Adresse der Website oder des Netzwerks ein, und wählen Sie ein Zertifikat aus.

Zertifikat, die in zertifikatbasierten Anmeldeinformationen verwendet werden sollen, müssen im privaten Speicher in der Zertifikatsverwaltung gespeichert werden.

Zertifikat-Manager öffnen

Internet- oder Netzwerkadresse (z. B. myserver, server.company.com)

Benutzername

Kennwort

Zertifikat auswählen

Systemsteuerung > Anmelde... > Windows-Anmeldeinformationen hinzufügen

Geben Sie die Adresse der Website oder des Netzwerks und Ihre Anmeldeinformationen ein.

Stellen Sie sicher, dass der eingegebene Benutzername und das eingegebene Kennwort für den Zugriff auf den ID verwendet werden können.

Internet- oder Netzwerkadresse (z. B. myserver, server.company.com)

Benutzername

Kennwort

Grundsätzlich stehen zwei Arten von Benutzerkonten zur Verfügung (diese Variante ist an Windows 7 Home angelehnt):

- **Administratoren:** dürfen „alles“
- **Standardbenutzer:** dürfen keine Programminstallationen durchführen, keine Netzwerkeinstellungen ändern etc.

Systemsteuerung > Benutzerkonten > Eigenen Kontotyp ändern

Wählen Sie den neuen Kontotyp aus

Christian Administrator Kennwortgeschützt

Sie müssen mindestens einem anderen Benutzer dieses Computers ein Administratorkonto zuweisen, bevor Sie den Typ dieses Benutzerkontos ändern können. Dadurch wird sichergestellt, dass mindestens eine Person oder ein Administratorkonto auf diesem Computer verfügt.

Standardbenutzer

Standardbenutzer können den Großteil der Software verwenden und die Systeminstellungen ändern, soweit dies keine Auswirkungen auf andere Benutzer bzw. die Sicherheit des Computers hat.

Administrator

Administratoren haben Vollzugriff auf den Computer und können beliebige Änderungen vornehmen. Basierend auf den Berechtigungsinstellungen werden Administratoren möglicherweise zum Eingeben ihres Kennworts und zum Bestätigen der anzuführenden Aktion aufgefordert, bevor die Änderungen vorgenommen, die Auswirkungen auf andere Benutzer haben.

Es wird empfohlen, dass Sie jedes Konto mit einem sicheren Kennwort schützen.

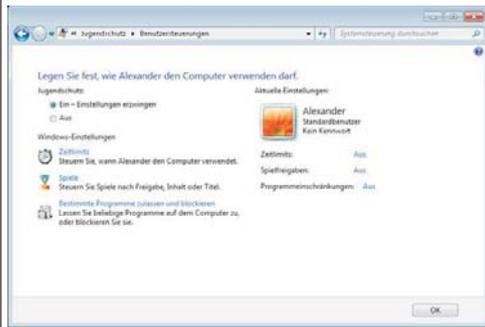
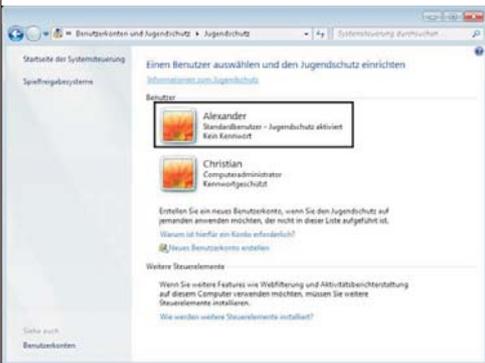
Warum ist ein Standardkonto empfehlenswert?

Kontotyp ändern

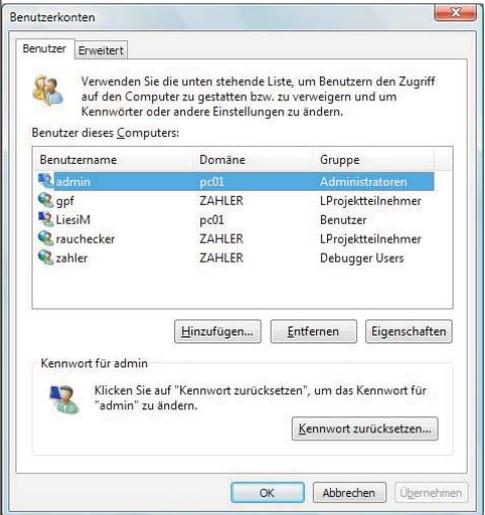
Abbrechen

Die Option **„Jugendschutz“** ermöglicht es, für bestimmte lokale Benutzerkonten zusätzliche Einschränkungen zu definieren:

Jugendschutz-Einstellungen sind nicht bei Domänen- und Administratoren-Konten möglich.



Ist der PC Mitglied einer Domäne, so wird der Systemsteuerungspunkt „Benutzerkonten“ geändert, sodass folgendes Bild eingeblendet wird:



**5.4 UAC (Benutzerkontosteuerung, User Account Control)**

Die Benutzerkontosteuerung wurde mit Windows Vista eingeführt. Sie ermöglicht eine Abwägung zwischen der Flexibilität und dem Berechtigungsumfang eines Administratorkontos und der Sicherheit eines Standardbenutzerkontos.

Wenn Sie eine administrative Aufgabe ausführen möchten, wie z. B. die Installation eines neuen Programms, fordert sind "elevated privileges" notwendig. Die UAC "dimmt" den Bildschirm und fordert Sie zur Bestätigung auf, dass Sie das Programm installieren möchten, bevor Sie diese administrativen Aufgaben ausführen können. Auf diese Weise wird die Verwendung von Administratorberechtigungen minimiert, wodurch es für bössartige Software (Malware) wie Viren, Würmer, Spyware und andere potenziell unerwünschte Programme schwieriger wird, den PC weitreichend zu befehlen.

In Windows 7 kann das Verhalten der Benutzerkontosteuerung fein abgestimmt werden.

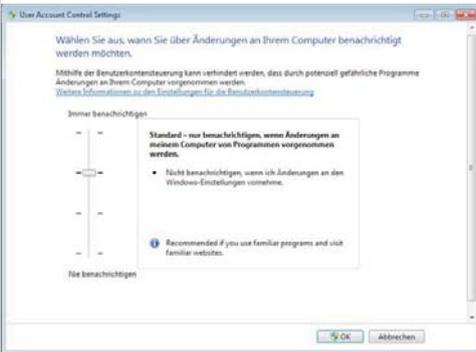


Öffnen Sie dazu die Systemsteuerung und navigieren Sie in das Menü "System und Sicherheit".



Es gibt nun vier Sicherheitsebenen:

- Immer benachrichtigen
- Standard – nur benachrichtigen, wenn Änderungen an meinem Computer von Programmen (nicht vom User selbst) vorgenommen werden
- nur benachrichtigen, wenn Änderungen an meinem Computer von Programmen (nicht vom User selbst) vorgenommen werden sowie Desktop nicht abblenden ("dimmen")
- Nie benachrichtigen



Der Benutzerkontoschutz dient auch dem Schutz der Computer von Familienmitgliedern vor Malware. Malware ist häufig in Programmen versteckt, die für Kinder reizvoll sind. Um Ihren Computer abzusichern, können Sie für Ihre Kinder Standardbenutzerkonten erstellen. Wenn Ihr Kind versucht, eine Softwarekomponente zu installieren, fordert das System die Eingabe des Kennworts eines Administratorkontos an. Dadurch können Ihre Kinder neue Programme nicht selbständig installieren.



**Technischer Hintergrund** (ausführlich in MOC 5949A, Unterrichtseinheit 6, S. 6-6 bis 6-17 erläutert):

In Windows 7 werden zwei Sicherheitstoken für ein Administratorkonto erzeugt. Die Verwendung des Administratorkontos muss autorisiert werden.

**5.4.1 Steuerung der UAC**

Das Verhalten der UAC kann mit Hilfe von Gruppenrichtlinien gesteuert werden. Diese Richtlinien können sowohl lokal als auch in der Domäne konfiguriert werden.



**5.4.2 Konfigurieren der UAC über die Registry**

Über die Registry kann das Standardverhalten der UAC für Administratoren und für Standardbenutzer konfiguriert werden.

Im Schlüssel

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System befinden sich drei dafür vorgesehene Einträge vom Typ REG\_DWORD:

- ConsentPromptBehaviorAdmin (Standardwert 5)
- ConsentPromptBehaviorUser (Standardwert 3)
- EnableLUA (Standardwert 1)

Name	Typ	Daten
ConsentPromptBehaviorAdmin	REG_DWORD	0x00000000 (0)
ConsentPromptBehaviorUser	REG_DWORD	0x00000003 (3)
EnableLUA	REG_DWORD	0x00000001 (1)

Die beiden ConsentPromptBehavior-Einträge können folgende folgende Werte annehmen:

- 0 Keine Aufforderungen mehr seitens der Benutzerkontensteuerung - alle Programme werden mit höheren Rechten ausgeführt
- 5 "Lockerste" Einstellung
- 2 "Strengste" Einstellung

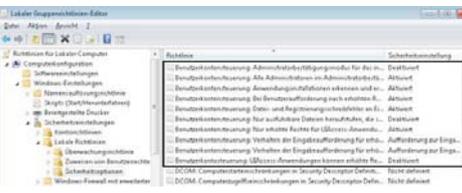
Der Wert EnableLUA muss auf 0 gesetzt werden, um die UAC auszuschalten.

Achtung

Aus Sicherheitsgründen sollte davon abgesehen werden, die Benutzerkontensteuerung auf dem Weg der Registry zu beeinflussen.

**5.4.3 Konfigurieren der UAC über lokale Gruppenrichtlinien**

Natürlich ist es auch möglich, das Verhalten der UAC über lokale GPO-Einstellungen zu beeinflussen:



**5.5 Netzwerkerkennung und Freigaben**

Um Ordner, Drucker und Dateien im Netzwerk gemeinsam verwenden zu können, ist die Einrichtung von Freigaben nötig.

**5.5.1 SMB (Server Message Blocks), auch: CIFS (Common Internet File System)**

Voraussetzung für die Verwendung freigegebener Ordner ist das SMB-Protokoll. SMB 1.0 wurde 1996 eingeführt. Es besteht aus einer Client- und einer Serverkomponente:

- **SMB-Serverdienst** (Dienstname: lanmanserver, Anzeigename: Server): wird benötigt, um Freigaben zu erstellen
- **SMB-Clientdienst** (Dienstname: lanmanworkstation, Anzeigename: Arbeitsstationsdienst) wird benötigt, um auf frei-

http://www.microsoft.com/windows/windows-7/

CLUBSYSTEM.NET

gegebenen Ordner und Drucker zugreifen zu können

In TCP/IP-Netzwerken lief SMB ursprünglich über den NetBIOS-Port 139, und die Namensauflösung erfolgte mittels WINS. In der Zwischenzeit wurde auch DNS als Namensauflösungsmechanismus hinzugefügt, der aber unter SMB 1.0 nur verwendet wird, wenn NetBIOS-Namen nicht verfügbar sind. Zurzeit läuft SMB auch als Dienst microsoft-ds über den Port TCP/UDP 445.

Seit Windows Vista und Windows Server 2008 wird SMB 2.0 mit folgenden Verbesserungen verwendet:

- Im selben Paket können mehrere SMB-Befehle übertragen werden. Das reduziert die Anzahl der SMB-Pakete.
- SMB 2.0 ist besser skalierbar.
- SMB 2.0 unterstützt symbolische Verknüpfungen.

Natürlich wird die bisherige Version SMB 1.0 nach wie vor weiter unterstützt.

Freigaben dürfen von Administratoren und Benutzern durchgeführt werden (beim Server auch Server-Operatoren).

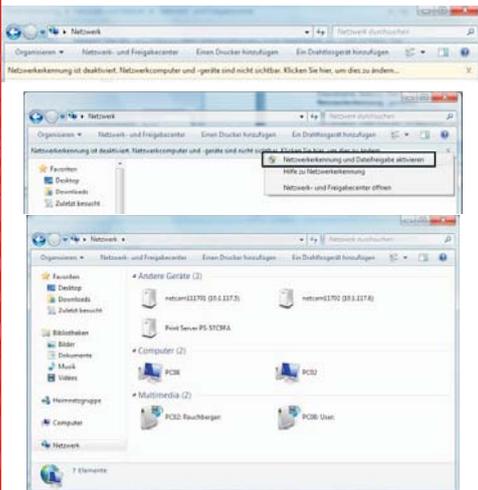
### 5.5 Netzwerkerkennung

In den Windows-Betriebssystemen von Windows for Workgroups 3.11 bis Windows XP/Server 2003 gab es einen Netzwerkdienst, der die Aufgabe hatte, Computer im Netzwerk zu erkennen. Dieser Dienst hatte den Namen **ComputerBrowser** (Dienstname: *Browser*) und arbeitete mit NetBIOS-Namensbroadcasts.

Obwohl der Dienst aus Gründen der Abwärtskompatibilität auch in Windows 7 noch enthalten ist, wurde eine völlig neues Protokoll entwickelt, das nun für diese Aufgaben zuständig ist: die Verbindungsschicht-Topologieerkennung (engl. *Link Layer Topology Discovery*, LLTD; Dienstname: *lltdsvc*). Der LLTD-Dienst ist zwar standardmäßig installiert, wird aber nur bei aktivierter Netzwerkerkennung gestartet.

Um von einem Windows XP- bzw. Server 2003-PC aus Windows Vista-/Windows 7-/Windows Server 2008-PCs in der Netzwerkübersicht sehen zu können, müssen Sie das Verbindungsschicht-Topologieerkennung-Antwortprogramm (LLTD Responder) für Windows XP separat downloaden und installieren (KB 922120).

Windows 7 deaktiviert im Profil „Arbeitsplatz“ standardmäßig die Netzwerkerkennung (das Auffinden von anderen SMB-Servern im Netzwerk) und die Dateifreigabe. Diese Einstellungen können wie folgt geändert werden:

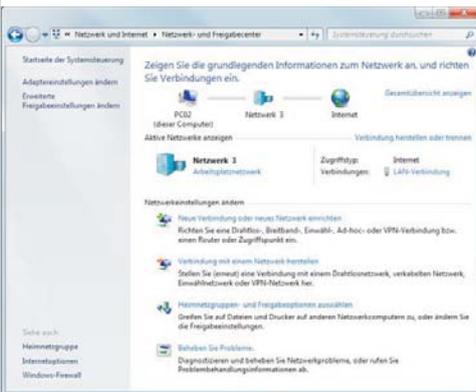


Für den problemlosen Peer-to-Peer-Netzwerkbetrieb (Arbeitsgruppenbetrieb) gibt es seit Windows 7 eine Reihe von neuen Diensten:

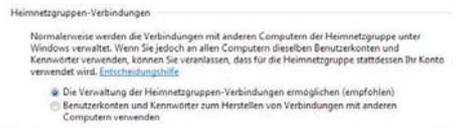
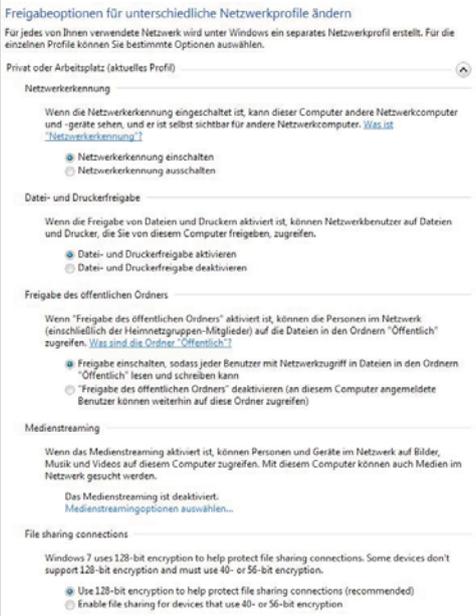
Anzeigename	Dienstname	Aufgabe
PeerNameResolution-Protokoll	PNRPsvc	Aktiviert die serverlose Peernamenauflösung (ohne DNS-Server) über das Internet. Falls dieser Dienst deaktiviert ist, können einige Peer-zu-Peer- und Zusammenarbeitsanwendungen, wie etwa „Windows-Teamarbeit“ und Filesharing-Applikationen, eventuell nicht ausgeführt werden.
Peernetzwerk-Gruppenzuordnung	p2psvc	Dieser Dienst ist für die Gruppenzuordnungen bei Peer-to-Peer Netzwerken unter Verwendung des IPv6-Protokolls zuständig. Ohne diesen Dienst kann es bei der Anwendung "Windows-Teamarbeit" zu Problemen kommen.
Peernetzwerkidentitäts-Manager	p2pimsvc	Dieser Dienst ist für die Identifizierung von Peer-to-Peer Netzwerken unter Verwendung des IPv6-Protokolls zuständig. Ohne diesen Dienst kann es bei der Anwendung "Windows-Teamarbeit" zu Problemen kommen.
PNRP-Computernamen veröffentlichte-Dienst	PNRPAutoReg	Dieser Dienst veröffentlicht einen Computernamen mit dem Peer Name Resolution-Protokoll. Die Konfiguration wird über den netsh-Kontext "p2p pnrp peer" verwaltet. Dieser Dienst unterstützt zwar auch IPv4, ist aber in erster Linie für den Einsatz unter IPv6 gedacht.

### Netzwerk- und Freigabecenter

In diesem Tool können die Freigabe- und Erkennungseinstellungen generell konfiguriert werden:



Unter Windows 7 gibt es unter „Erweiterte Freigabeeinstellungen ändern“ die Möglichkeit, eine Vielzahl von Konfigurationseinstellungen zu treffen:



### 5.6 Benutzerprofile

In Benutzerprofilen sind benutzerdefinierte Desktopumgebungen definiert. Dazu gehören individuelle Einstellungen für die Anzeige, Netzwerk- und Druckerverbindungen sowie weitere festgelegte Einstellungen. Ihre Desktopumgebung kann vom Benutzer selbst oder vom Systemadministrator eingerichtet werden. Technisch gesehen handelt es sich bei Benutzerprofilen um Unterordner von C:\Benutzer (bis Windows XP „C:\Dokumente und Einstellungen“), wobei folgende Komponenten das Profil bilden:

- Benutzer
  - All Users
  - Christian
  - Anwendungsdaten
  - AppData
  - Cookies
  - Desktop
  - Downloads
  - Druckumgebung
  - Eigene Bilder
  - Eigene Dateien
  - Eigene Dokumente
  - Eigene Musik
  - Eigene Videos
  - Favoriten
  - Gespeicherte Spiele
  - Kontakte
  - Links
  - Lokale Einstellungen
  - Netzwerkumgebung
  - Recent
  - SendTo
  - Startmenü
  - Suchvorgänge
  - Vorlagen

● Die Datei NTUSER.DAT stellt einen Teil der Registry dar und enthält benutzerdefinierte Systemeinstellungen.

● Eine Reihe von Ordnern enthalten benutzerdefinierte Dateien; bekannt sind etwa die Ordner „Dokumente“ oder „Desktop“.

Das Profil „Default“ stellt eine Vorlage dar, die beim erstmaligen Anmelden eines Benutzers kopiert wird und den Ausgangsstatus für das neue Benutzerprofil bildet.

Das Profil „All Users“ gibt es eigentlich nicht mehr; es stellt nur mehr einen System-Link zum Verzeichnis c:\ProgramData dar. Dieses Verzeichnis enthält die Startmenüdateien für „alle Benutzer“ in folgendem Pfad:

```
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
```

Neu sind Einträge, die keinen echten Ordner darstellen. Sie sind mit einem Verknüpfungssymbol (kleiner schwarzer, nach rechts oben weisender Pfeil) gekennzeichnet, zum Beispiel.

Auf solche Verknüpfungen kann in den meisten Fällen nicht direkt zugegriffen werden, da sie in Wirklichkeit nur eine **Verbindung** (engl. *Junction*) zu einem anderen Ordner darstellen.

**Hinweis:** Junctions werden nur sichtbar, wenn in den Ordneroptionen in der Karteikarte „Ansicht“ die Einstellung „Geschützte Systemdateien ausblenden“ deaktiviert wird.

**Beispiel:** Ein Klick auf den Verweis

Cookies führt zur Meldung:



Um nun herauszufinden, auf welchen Ordner eine Verbindung zeigt, kann der Command-Shell-Befehl `dir /a` verwendet werden:

```
C:\Users>dir /a
Volume in Laufwerk C: hat keine Bezeichnung.
Volumeseriennummer: 7448-CE17
Verzeichnis von C:\Users
26.05.2009 11:04 <DIR> .
26.05.2009 11:04 <DIR> ..
22.04.2009 10:27 <SYMLINKD> All Users [C:\ProgramData]
11.06.2009 09:16 <DIR> Christian
26.05.2009 11:04 <DIR> Default
22.04.2009 10:27 <VERBINDUNG> Default User [C:\Users\Default]
22.04.2009 10:14 174 desktop.ini
22.04.2009 13:07 <DIR> Public
1 Datei(en), 174 Bytes
7 Verzeichnis(se), 24.596.566.016 Bytes frei
```

Beachten Sie die Kennzeichnung des „All Users“-Profils als System-Link!

```
C:\Users\Christian>dir /a
Volume in Laufwerk C: hat keine Bezeichnung.
Volumeseriennummer: 7448-CE17
Verzeichnis von C:\Users\Christian
11.06.2009 09:16 <DIR> .
11.06.2009 09:16 <DIR> ..
26.05.2009 11:04 <VERBINDUNG> Anwendungsdaten [C:\Users\Christian\AppData\Roaming]
26.05.2009 11:04 <DIR> AppData
26.05.2009 11:05 <DIR> Contacts
26.05.2009 11:04 <VERBINDUNG> Cookies
[C:\Users\Christian\AppData\Roaming\Microsoft\Windows\Cookies]
12.06.2009 16:58 <DIR> Desktop
12.06.2009 16:55 <DIR> Documents
26.05.2009 11:49 <DIR> Downloads
26.05.2009 11:04 <VERBINDUNG> Druckumgebung
[C:\Users\Christian\AppData\Roaming\Microsoft\Windows\Printer Shortcuts]
26.05.2009 11:04 <VERBINDUNG> Eigene Dateien [C:\Users\Christian\Documents]
```

Hier sehen Sie, dass es sich beim Ordner Cookies um eine Verbindung (Junction) auf den tatsächlich existierenden Ordner `C:\Users\Christian\AppData\Roaming\Microsoft\Windows\Cookies` handelt. In diesen Ordner können Sie im Explorer ohne Berechtigungsprobleme hineinschauen.

Einige wichtige Ordner im Benutzerprofil:

● „Desktop“: Dieser Ordner enthält Dateien, die am Desktop gespeichert sind.

● „Documents“, „Pictures“, „Music“, „Videos“: Dieser Ordner enthält Dateien, die in einer der vier Standardbibliotheken gespeichert sind.

● „Download“: Dieser Ordner ist ein Standard-speicherort für aus dem Internet heruntergeladene Dateien.

● „Favoriten“: Dieser Ordner enthält Verknüpfungen zu bevorzugten Websites, Dateien und Verzeichnissen.

● „Appdata“: Dieser Ordner enthält verschiedene Anwendungsdaten, sortiert nach Position und Verwendung.

- Der Ordner „Local“ enthält lokal gespeicherte Informationen.
- Der Ordner „LocalLow“
- Der Ordner „Roaming“ enthält die servergespeicherten Anteile des Profils.

● „AppData\Local\Microsoft“: In diesem Ordner sind unter anderem auch die lokalen Mail-Datenbanken gespeichert, die alle eingegangenen und gesendeten E-Mails, alle Kontakte und auch die Terminpläne enthalten, die in Outlook bzw. Windows Mail (Nachfolger von Outlook Express) gespeichert sind.

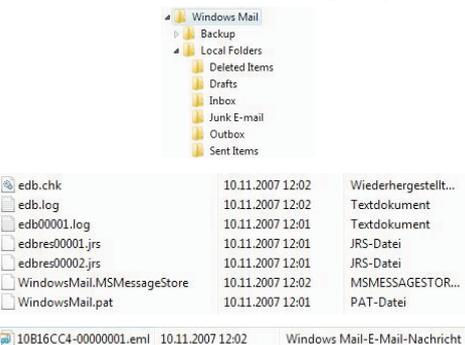
● „AppData\Local\Microsoft\Outlook“: In Outlook wird dafür (wenn kein Postfach auf einem Exchange Server konfiguriert ist) eine einzige Datenbankdatei mit dem Namen `outlook.pst` verwendet. Der Pfad zu dieser Datei lautet zum Beispiel:

```
C:\Users\Benutzername\AppData\Local\Microsoft\Outlook\outlook.pst
```



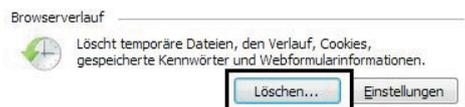
● „AppData\Local\Microsoft\Windows Mail“: Von Windows Mail wird eine komplette Ordnerstruktur erzeugt. Die Nachrichten landen im `Windows.MSMessageStore`, werden aber innerhalb

der einzelnen Mailordner (etwa „Inbox“) noch einmal als \*.eml (E-Mail-Datei) angezeigt.



● „AppData\Local\Temp“ enthält temporäre Dateien, die von Anwendungsprogrammen oder Diensten während der Laufzeit erzeugt werden (beispielsweise bei der Installation neuer Software). Er sollte immer leer sein.

„AppData\Local\Microsoft\Windows\Temporary Internet Files“: stellt den Webcache des Internet Explorers dar. In ihm werden alle besuchten Websites und dazu nötige Cookies zwischengespeichert. Auch dieser Ordner sollte regelmäßig gelöscht werden. Das Löschen dieses Ordners ist auch über das Menü [Extras] – [Internetoptionen], Karteikarte „Allgemein“ möglich:



In folgendem Dialogfeld können temporäre Dateien, die während des Surfens gespeichert wurden, gelöscht werden:



● „AppData\Local\Microsoft\Windows\History“ (Verlauf): Hier speichert der Internet Explorer Links zu besuchten Websites.

● „AppData\Roaming\Microsoft\Windows\Cookies“: Unter Cookies versteht man kleine Textdateien, die beim Anwählen bestimmter Internetsites lokal gespeichert werden und zum Datenaustausch zwischen Client und Server dienen. In Cookies können persönliche Vorlieben, Datum und Zeit des letzten Besuchs oder Benutzernamen und Kennwörter gespeichert werden.

zähler@amazon[5].txt	01.11.2007 21:10	Textdokument	1 KB
zähler@derstandard[1]...	07.10.2007 19:25	Textdokument	1 KB
zähler@doubliclick[1]...	05.11.2007 22:44	Textdokument	1 KB
zähler@microsoft[1].txt	26.08.2007 12:58	Textdokument	1 KB

http://www.microsoft.com/windows/windows-7/

CLUBSYSTEM.NET

● **„AppData\Roaming\Microsoft\Windows\Start Menu“** (Startmenü): Dieser Ordner enthält Verknüpfungen zu Programmen, die im Startmenü – zusammengefasst in Gruppen – angezeigt werden.

● **„AppData\Roaming\Microsoft\Windows\Recent“** (Zuletzt verwendete Dokumente): Dieser Ordner enthält Verknüpfungen zu Dokumenten und Ordnern, die in der letzten Zeit vom Benutzer verwendet wurden. Diese Verknüpfungen werden an der entsprechenden Stelle im Startmenü angezeigt.

**Typen von Benutzerprofilen**

**Lokales Benutzerprofil:** Das lokale Benutzerprofil wird beim ersten Anmelden bei einem Computer erstellt und auf der lokalen Festplatte des betreffenden Computers gespeichert. Sämtliche Änderungen an Ihrem lokalen Benutzerprofil sind nur für den Computer wirksam, auf dem die Änderungen vorgenommen wurden.

● **Servergespeichertes Benutzerprofil:** Das servergespeicherte Benutzerprofil wird vom Systemadministrator erstellt und auf einem Server gespeichert. Dieses Profil steht immer zur Verfügung, wenn Sie sich an einem Computer im Netzwerk anmelden. An Ihrem servergespeicherten Benutzerprofil vorgenommene Änderungen werden auf dem Server aktualisiert. Voraussetzung ist die Verwendung einer Active Directory-Domäne.

● **Verbindliches Benutzerprofil:** Das verbindliche Benutzerprofil ist ebenfalls ein servergespeichertes Profil, mit dessen Hilfe bestimmte Einstellungen für einzelne Benutzer oder einer Benutzergruppe festgelegt werden können. Änderungen an den verbindlichen Benutzerprofilen können lediglich von den Systemadministratoren vorgenommen werden. Verbindliche Benutzerprofile erhält man, indem die Datei NTUSER.DAT in NTUSER.MAN (für „mandatory“) umbenannt wird. Diese Technologie sollte heute nicht mehr verwendet werden; sie wurde durch Gruppenrichtlinienobjekte ersetzt.

● **Temporäres Benutzerprofil:** Ein temporäres Profil wird in jeder Situation ausgegeben, in der durch eine Fehlerbedingung das Laden des Benutzerprofils verhindert wird. Temporäre Profile werden am Ende einer Sitzung gelöscht. Änderungen, die der Benutzer an den Desktopeinstellungen und Dateien vorgenommen hat, gehen beim Abmelden des Benutzers verloren. Hinweis: Der Benutzer „Gast“ erhält stets ein temporäres Benutzerprofil!

**Kopieren von Benutzerprofilen**

Benutzerprofile können dupliziert und lokal gelöscht werden; dafür steht das Dialogfeld „Systemeigenschaften“ zur Verfügung (erreichbar über das Kontextmenü des Arbeitsplatzes oder über Systemsteuerung – System):

Mit der Schaltfläche „Typ ändern“ kann ein servergespeichertes Profil in ein lokales geändert werden (nicht umgekehrt!).

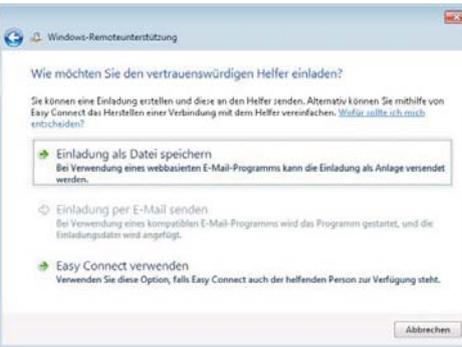
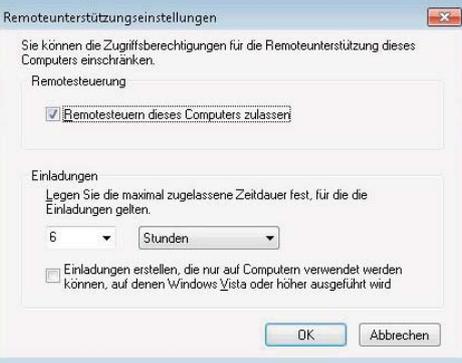
**5.7 Remoteunterstützung**

Hier gibt es die neue Möglichkeit „Easy Connect“, die aber erweiterte Features bei den verwendeten Routern voraussetzt.

Schalten Sie zunächst in den Systemeigenschaften die Remoteunterstützung frei.

Für EasyConnect müssen beiden Computer Windows 7 ausführen und PNRP unterstützen (Peer Name Resolution Protocol), die verwendeten

Router müssen IPv6-Tunneling und UPnP unterstützen. Ob Ihre Router für EasyConnect ge-

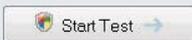


eignet sind, können Sie mit einem Microsoft-Tool überprüfen, das über folgende URL erreichbar ist:

<http://www.microsoft.com/windows/using/tools/igd/default.msp>

**Internet Connectivity Evaluation Tool**

Click the button below to start the tests.  
More Information ...



**5.8 Microsoft SharedView**

Das unter Windows Vista vorhandene Feature "Windows Teamarbeit" wurde in Windows 7 durch Microsoft SharedView ersetzt. Es ist damit möglich, Besprechungen einzurichten und Dokumente oder Programme für bis zu 15 Personen freizugeben. Der wichtigste Unterschied zwischen den beiden ist die Erweiterung der Funktionalität von dem internen Netzwerk aufs Internet durch das Benutzen des HTTP Protokolls. Um Meetings zu erstellen oder beizutreten, ist ein LiveID-Konto erforderlich.

SharedView muss von der Microsoft-Homepage heruntergeladen werden.

Unterstützt werden grundsätzlich 32 bit-Betriebssysteme ab Windows Vista; obwohl es

derzeit (Stand: Juni 2009) noch keine offizielle Unterstützung von 64 bit-Plattformen gibt, existieren Workarounds dafür.

Um eine neue Sitzung zu starten, melden Sie sich mit Ihrer LiveID an.



Dann klicken Sie auf "Sitzung starten":



Durch Klicken auf "Neue Sitzung starten"

Wenn Sie andere Personen einladen möchten, senden Sie diesen folgende Anweisungen:

office@zahler.at hat Sie eingeladen, einer Online-Arbeitsitzung mit SharedView beizutreten.

So treten Sie einer Sitzung bei:

- Klicken Sie auf folgenden Link: [https://joinsvw.sharedview.com/join.aspx?ID=office@zahler.at&pass=7LURA\\$6L](https://joinsvw.sharedview.com/join.aspx?ID=office@zahler.at&pass=7LURA$6L)
- Öffnen Sie SharedView. Treten Sie der Sitzung bei, indem Sie Folgendes eingeben:  
Sitzungsname: office@zahler.at  
Kennwort: 7LURA\$6L

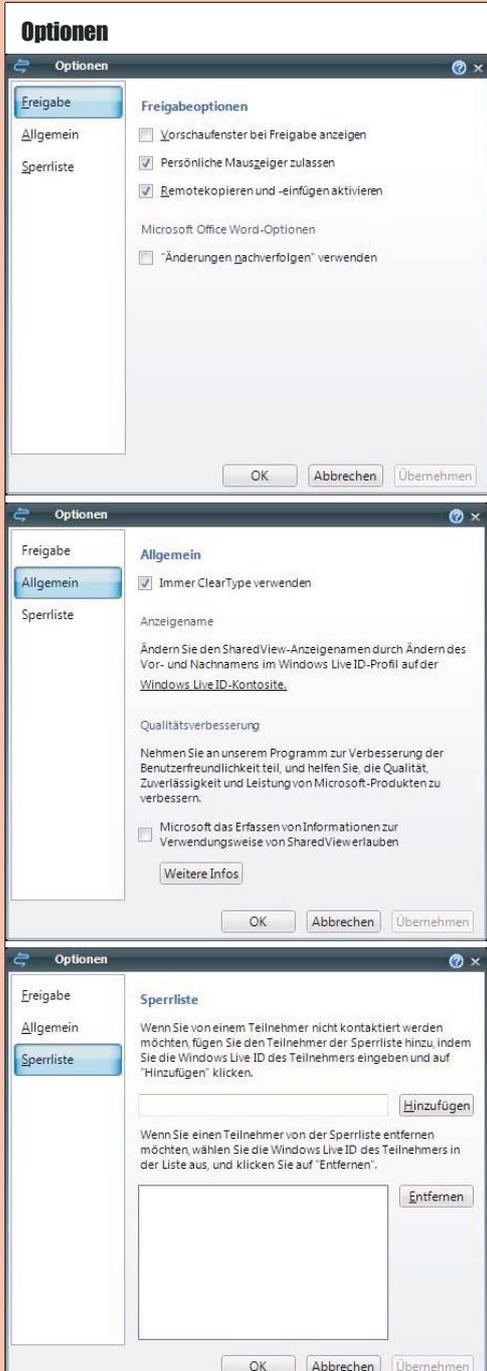
Hilfe und ausführlichere Anweisungen finden Sie unter:  
[http://r.office.microsoft.com/r/rldsv?clid=1031&p1=1&p2=Instructions\\_S2](http://r.office.microsoft.com/r/rldsv?clid=1031&p1=1&p2=Instructions_S2)

Anweisungen in die Zwischenablage kopieren



Um die Sitzung zu erstellen, klicken Sie auf "Start".

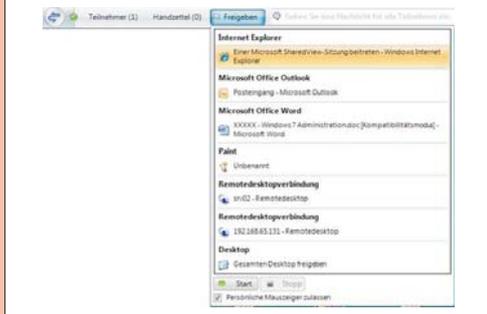




Beitreten zu einer SharedView-Sitzung:  
Geben Sie die in den Anweisungen enthaltene URL im Internet Explorer ein:



Sitzungsteilnehmer können nun den gesamten Desktop, Programme oder Daten für andere Teilnehmer freigeben:



Wenn jemand einer Sitzung beitreten möchte, so wird das folgendermaßen angezeigt:



## 6 Drucker und Geräte

Im Startmenü gibt es einen neuen Menüpunkt „Geräte und Drucker“:



Zuordnen von Druckern zu Netzwerkstandorten: Dieses Feature ist neu unter Windows 7.



## 7 Datenträgerverwaltung, Startvorgang und Notfallwiederherstellung

### 7.1 Booten von VHD

Ein neues Feature von Windows 7 ist die Möglichkeit, direkt von einer virtuellen Festplatte (VHD) zu booten.

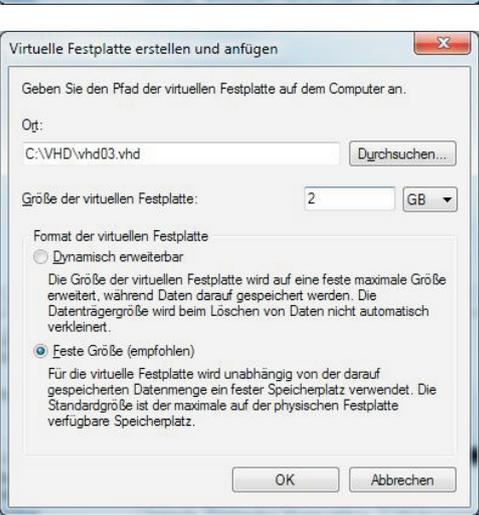
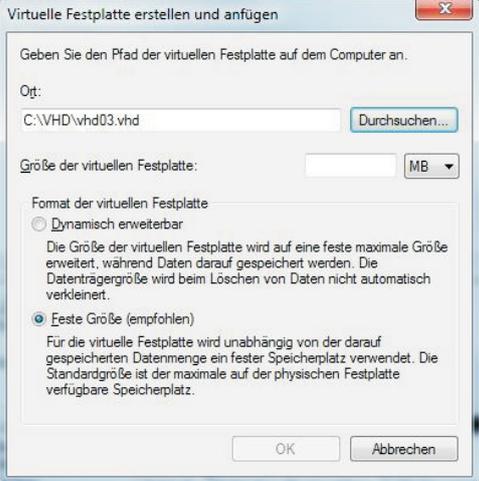
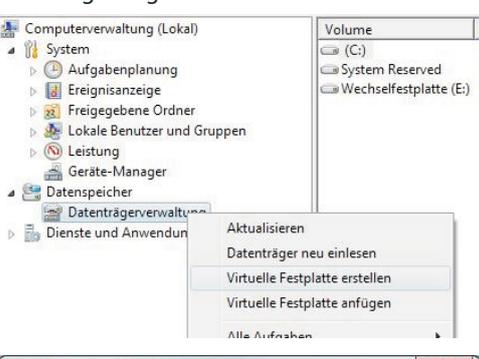
In Windows® 7 können virtuelle Festplatten als ausgeführtes Betriebssystem auf designierter Hardware ohne ein anderes, übergeordnetes Betriebssystem, einen virtuellen Computer oder Hypervisor verwendet werden. VHD-Dateien können mit den Windows 7-Datenträgerverwaltungstools erstellt werden, d. h. mit dem Befehlszeilentool *DiskPart* und dem MMC-Snap-In (*Microsoft Management Console*) für die Datenträgerverwaltung. Eine Windows 7-Abbilddatei (WIM-Format) kann für die virtuelle Festplatte bereitgestellt werden, und die VHD-Datei kann auf mehrere Systeme kopiert werden. Der Windows 7-Start-Manager kann für den systemeigenen, oder physikalischen, Start des Windows-Abbilds auf der virtuellen Festplatte konfiguriert werden. Die VHD-Datei kann außerdem für die Verwendung mit der Rolle für Hyper-V in Windows Server® 2008 R2 mit einem virtuellen Computer verbunden werden. Es ist nicht vorgesehen, dass VHD-Dateien für den systemeigenen Start die vollständige Abbildbereitstellung auf allen Client- oder Serversystemen ersetzen. In früheren Windows-Versionen wird das systemeigene Starten von einer virtuellen Festplatte nicht unterstützt. Zum Starten von einer VHD-Datei sind hier ein Hypervisor und ein virtueller Computer erforderlich.

Für die Schritte zum Bereitstellen eines Windows 7- oder Windows Server 2008 R2-Abbilds in einer VHD-Datei sind die Windows-Bereitstellungstools erforderlich, einschließlich *imagex.exe*. Mit *imagex.exe* wird eine Windows-Betriebssystempartition im Windows Image-Dateiformat (WIM) erfasst, und es wird eine WIM-Datei auf eine Dateisystempartition angewendet, die sich in einer VHD-Datei befinden kann.

Für den systemeigenen Start von Windows 7 aus einer VHD-Datei ist auch die Windows 7-Startumgebung erforderlich. Die Windows 7-Startumgebung wird bei der vollständigen Installation des Betriebssystems initialisiert und umfasst den Windows-Start-Manager und Startkonfigurationsdaten (*Boot Configuration Data, BCD*) sowie andere unterstützende Dateien.

### 7.1.1 Erstellen einer VHD auf grafischem Weg

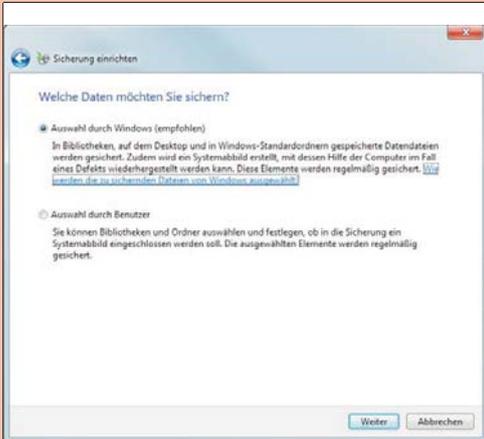
Eine virtuelle Festplatte (*virtual hard disk, VHD*) kann über das MMC-Snap-In Computerverwaltung erfolgreich.



http://www.microsoft.com/windows/windows-7/

CLUBSYSTEM.NET

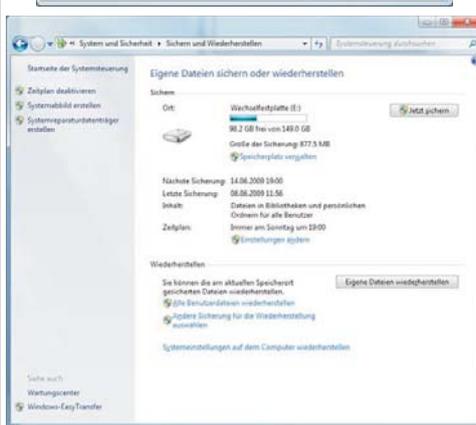
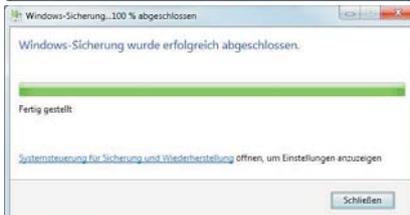
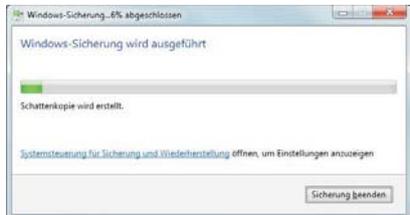
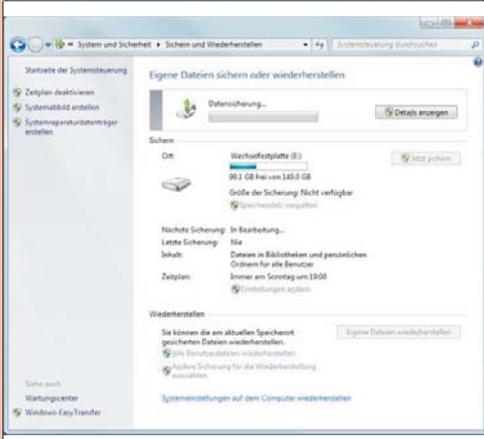
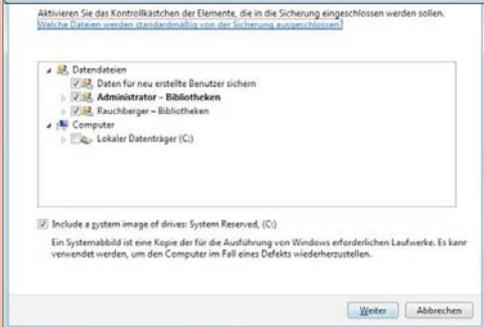
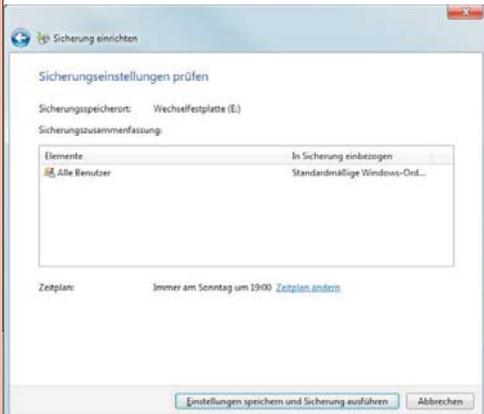




Bei „Auswahl durch Windows“ werden folgende Elemente gesichert:

- Bibliotheken: Alle Dateien, die sich in Bibliotheken befinden, vorausgesetzt, sie sind lokal gespeichert und das Laufwerk ist mit NTFS formatiert.
- Desktop: Alle Dateien, die sich auf dem Desktop befinden.
- System-Image: Falls genug Platz auf dem Sicherungsmedium vorhanden ist, wird ein System-Image mit dem gesamten Betriebssystem, allen Treibern, Registry-Einstellungen und installierten Softwareprodukten erstellt.

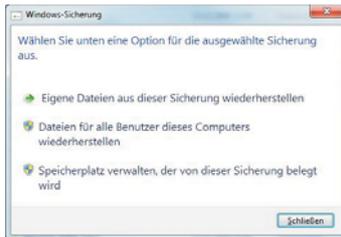
Bei „Auswahl durch Benutzer“ kann aus allen Ordnern selbst eine Auswahl getroffen werden:



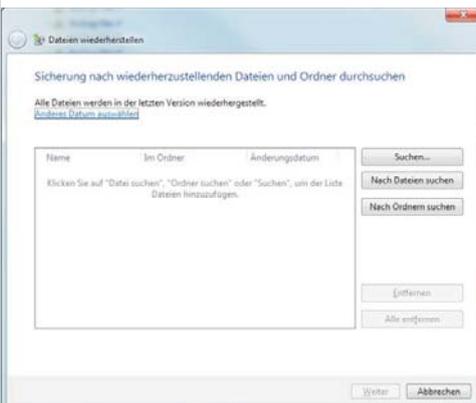
**Aufbau des Backup-Verzeichnisses**

- PC02
  - Backup Set 2009-06-08 115247
    - Backup Files 2009-06-08 115247
      - Backup files 1
      - Backup files 2
      - Backup files 3
      - Backup files 4
      - Backup files 5
      - Backup files 6
      - Backup files 7
      - Catalogs

Klickt man doppelt auf den PC-Namen, so erscheint folgendes Menü:



Auf diese Art ist es möglich, einige oder alle Dateien aus der durchgeführten Sicherung wiederherzustellen.



Außerdem ist es möglich, einen Systemreparatur-Datenträger zu erstellen:

**7.2.2 Startup Repair**

Entweder ist Booten von DVD nötig, dann auf



„Computerreparaturoptionen“ klicken.



Auf Grund der zusätzlichen Partition kann Windows 7 Startprobleme auch selbst erkennen und verzweigt dann automatisch in die Starthilfe-Tools.

Es werden dann die bestehenden Windows-Installationen gesucht:



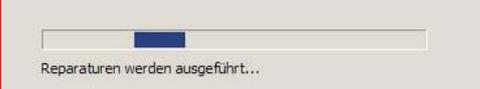
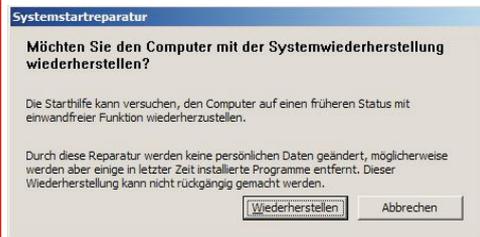
http://www.microsoft.com/windows/windows-7

CLUBSYSTEM.NET

Hier besteht über den Button "Treiber" auch die Möglichkeit, zusätzliche Treiber aus einer anderen Quelle zu laden. Nach der Auswahl der gewünschten Windows-Version wird ein neues Fenster geöffnet, welches die folgenden Möglichkeiten anbietet:



● **Systemstartreparatur:** Automatisches Reparieren von Windows Startproblemen (Bootsektor usw.)



● **Systemwiederherstellung:** Herstellen von Windows über vorhandene Wiederherstellungspunkte (Konfiguration von Wiederherstellungspunkten siehe nächstes Kapitel)

● **Systemabbild-Wiederherstellung:** Stellt das System mit Hilfe eines zuvor mit Windows Backup erstellten Systemabbilds wieder her.

● **Windows-Speicherdiagnosetool:** Arbeitsspeicher auf Fehler überprüfen (Neustart erforderlich)

● **Eingabeaufforderung** (bis Windows XP: „Wiederherstellungskonsole“): Kommandozeile/Eingabeaufforderung

**7.2.3 Systemwiederherstellung und Volumenschattenkopien („Volume Shadow Copies“)**

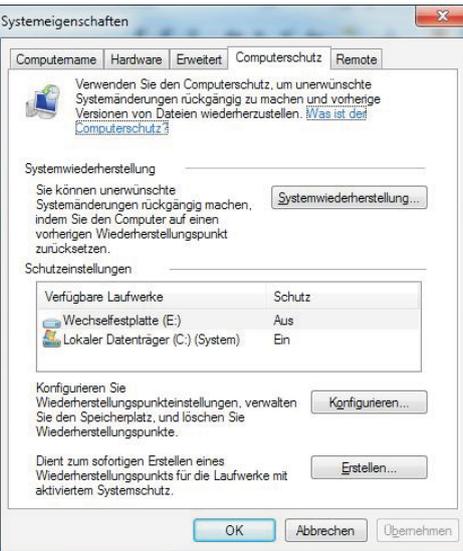
Die Systemwiederherstellung wurde unter Windows XP eingeführt, damit Benutzer ihre Computer in einen vorherigen Zustand zurückversetzen können, ohne persönliche Dateien zu verlieren (wie z. B. Microsoft Office Word-Dokumente, Grafikdateien und E-Mail-Nachrichten). Für die Systemwiederherstellung müssen keine Systemnapshots erstellt werden, da das System einfach erkennbar

re Wiederherstellungspunkte automatisch anlegt, mit deren Hilfe Sie Ihr System auf einen früheren Zeitpunkt zurücksetzen können. Wiederherstellungspunkte werden sowohl zum Zeitpunkt wichtiger Systemereignisse (z. B. bei der Installation von Anwendungen oder Treibern) als auch in regelmäßigen Abständen (täglich) erstellt. Sie können Wiederherstellungspunkte jederzeit erstellen und benennen.

Die Systemwiederherstellung unter Windows XP basiert auf einem Dateifilter, der Dateiänderungen für einen bestimmten Satz von Dateinamenerweiterungen überwacht und Dateien kopiert, bevor diese überschrieben werden. Wenn ein Problem auftritt, können Sie die Systemdateien und die Registrierung auf ein vorheriges Datum zurücksetzen, an dem das System bekanntermaßen ordnungsgemäß funktioniert hat.

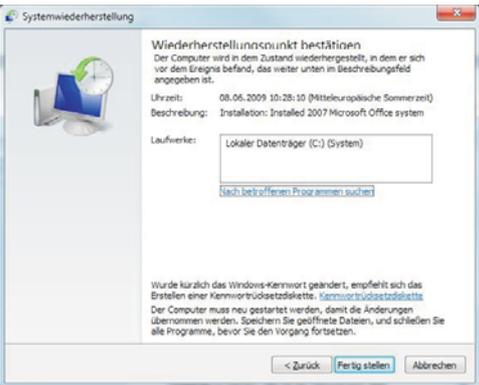
Unter Windows 7 ermöglicht die Systemwiederherstellung eine Wiederherstellung nach einer größeren Vielfalt von Änderungen als unter Windows XP. Das Dateifiltersystem für die Systemwiederherstellung in früheren Versionen von Windows wurde durch eine neue Methode ersetzt. Wenn nun ein Wiederherstellungspunkt erforderlich ist, wird eine Schattenkopie einer Datei oder eines Ordners erstellt. Eine Schattenkopie ist im Wesentlichen eine frühere Version der Datei oder des Ordners zu einem bestimmten Zeitpunkt. Windows 7 kann Wiederherstellungspunkte automatisch oder nach Aufforderung erstellen. Wenn das System wiederhergestellt werden muss, werden Dateien und Einstellungen aus der Schattenkopie auf das aktive von Windows 7 verwendete Volume kopiert. Dadurch wird die Integration mit anderen Aspekten der Sicherung und Wiederherstellung verbessert und die Systemwiederherstellungsfunktion noch nützlicher.

**Aktivieren des Computerschutzes:** Unter Systemeigenschaften – Computerschutz:



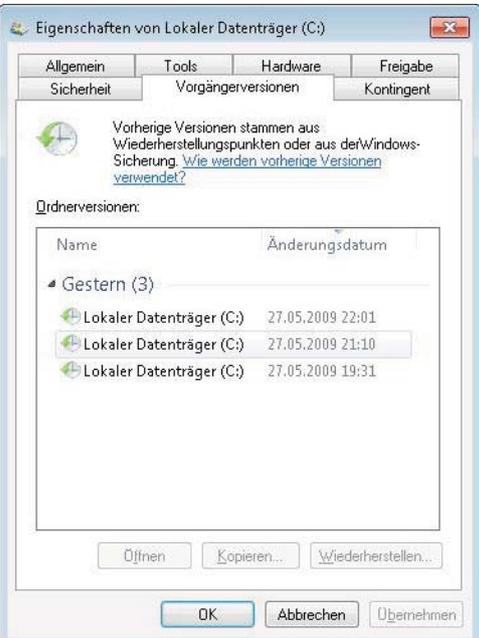
Schattenkopien werden automatisch als Teil eines Wiederherstellungspunkts in den Systemeigenschaften gespeichert. Wenn der Computerschutz aktiviert ist, erstellt Windows automatisch Schattenkopien von Dateien, die seit dem letzten Wiederherstellungspunkt, also in der Regel seit einem Tag, geändert wurden. Wenn die Festplatte partitioniert ist oder wenn mehrere Festplatten im Computer installiert sind, müssen Sie den Computerschutz

auch auf den anderen Partitionen oder Festplatten aktivieren.



Klicken Sie mit der rechten Maustaste auf die Datei bzw. den Ordner, und klicken Sie dann auf *Vorherige Versionen wiederherstellen*.

Es wird eine Liste der verfügbaren vorherigen Datei- oder Ordnerversionen angezeigt. Die Liste enthält sowohl Sicherungs- als auch Schattenkopien, sofern beide Typen vorhanden sind.



### 7.3 Problembehandlung

#### 7.3.1 Windows Troubleshooting Platform (WTP)

Die neue Windows Troubleshooting Platform verwendet Powershell-Scripts zur Analyse und Behebung computerbezogener Probleme.

Die WTP beinhaltet drei Komponenten:

- **Troubleshooting Packs:** Ein solches Paket besteht aus einer XML-Manifest-Datei, die die ursprünglichen Ursachen eines Zustands beschreiben, sowie aus Powershell-Scripts, die das Problem analysieren und gegebenenfalls lösen. Windows 7 enthält etwa 24 integrierte Pakete.
- **Troubleshooting Engine**
- **Troubleshooting Wizard:** Mit diesem Assistenten kann der Benutzer durch die einzelnen Schritte geführt werden, die ein *Troubleshooting Pack* benötigt.

#### 7.3.2 Problemaufzeichnung (Problem Steps Recorder)

Windows 7 enthält ein Tool mit dem Namen "Problem Steps Recorder", mit dem Benutzer ihre Aktionen als Folge von Screenshots aufzeichnen können.

Starten Sie das Tool, indem Sie in der Suche im Startmenü "record" eingeben:



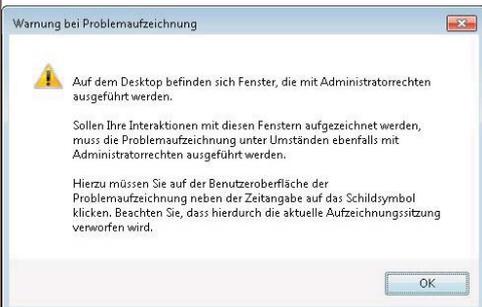
Systemsteuerung (1)

Schritte zum Reproduzieren eines Problems aufzeichnen

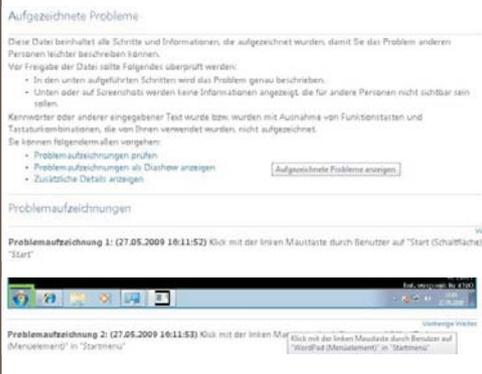
Der Recorder startet, mit "Aufzeichnung starten" wird die Aufzeichnung begonnen.



Nun wiederholt der Anwender genau die Schritte, die zu seinem Problem geführt haben, und beendet dann die Aufzeichnung.



Nach Beendigung der Aufzeichnung wird ein gezipptes MHT-Dokument erstellt (die folgende Abbildung stellt nur einen Ausschnitt aus einem derartigen Dokument dar):



Der folgende Abschnitt beinhaltet die zusätzlichen aufgetragenen Details, die zum Finden einer Lösung des Problems beitragen können.  
Diese Details ermöglichen die genaue Identifizierung der Programme und der Benutzeroberfläche, die bei der Problemaufzeichnung verwendet wurden.  
Dieser Abschnitt beinhaltet möglicherweise programminternen Text, der nur für besonders versierte Benutzer oder Programmierer verständlich ist.  
Prüfen Sie diese Details, um sicherzustellen, dass Sie keine Informationen beinhalten, die für andere nicht sichtbar sein sollen.  
Aufzeichnungszeitpunkt: 27.05.2009 16:11:34 - 16:12:22  
Problemaufzeichnung 1: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 2: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 3: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 4: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 5: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 6: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 7: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 8: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 9: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 10: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 11: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 12: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 13: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 14: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 15: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 16: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 17: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 18: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 19: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 20: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 21: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 22: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 23: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 24: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 25: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 26: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 27: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 28: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 29: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 30: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 31: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 32: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 33: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 34: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 35: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 36: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 37: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 38: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 39: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 40: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 41: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 42: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 43: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 44: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 45: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 46: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 47: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 48: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 49: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 50: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 51: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 52: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 53: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 54: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 55: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 56: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 57: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 58: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 59: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 60: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 61: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 62: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 63: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 64: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 65: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 66: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 67: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 68: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 69: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 70: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 71: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 72: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 73: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 74: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 75: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 76: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 77: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 78: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 79: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 80: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 81: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 82: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 83: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 84: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 85: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 86: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 87: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 88: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 89: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 90: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 91: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 92: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 93: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 94: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 95: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 96: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 97: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 98: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 99: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1  
Problemaufzeichnung 100: Klick mit der linken Maustaste durch Benutzer auf "Start (Schaltfläche)"  
Betrifft System: 7100.0.6002.x-wwan.win7en.090421-1700 x-1.0.0.2.1

### 7.4 DeviceStage

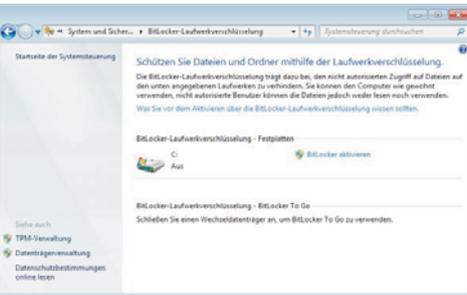
Ein neues Feature unter Windows 7 vereinfacht die Installation von Gerätetreibern. Wird ein mit Windows 7 kompatibles Gerät an den PC angeschlossen, so sehen Sie in "Device Stage" den aktuellen Gerätestatus und die Möglichkeiten, die Sie mit diesem Gerät haben.



## 8 Windows 7-Sicherheitseinstellungen

### 8.1 BitLocker Drive Encryption

Eine der größten Neuerungen im Business-Bereich ist die Verschlüsselungstechnik rund um **BitLocker**. Enthalten ist die neue Technologie in den Ultimate- und der Enterprise-Edition sowie der kommenden Server-Version. BitLocker verschlüsselt die Windows-Partition; dabei ist der Schutz bereits während des Bootvorgangs aktiv.



Hinweis: Für die Verschlüsselung weiterer Partitionen steht **EFS (Encrypting File System)** zur Verfügung.

**BitLocker Drive Encryption** wurde entworfen, um Endbenutzern einen bestmöglichen Umgang mit Systemen zu ermöglichen, die über einen kompatiblen TPM-Mikrochip und ein entsprechendes BIOS verfügen. Ein TPM gilt als kompatibel, wenn es ein TPM der Version 1.2 mit allen entsprechenden BIOS-Änderungen ist, die erforderlich sind, um die von der *Trusted Computing Group* definierte BIOS-Erweiterung *Static Root of Trust Measurement* zu unterstützen. Das TPM interagiert mit **BitLocker Drive Encryption**, um beim Systemstart nahtlosen Schutz zu bieten.

**BitLocker Drive Encryption** kann auch auf Computern ohne ein kompatibles TPM verwendet werden. In diesem Fall können Sie mit **BitLocker Drive Encryption** zwar die Funktionen zur Volumeverschlüsselung verwenden, Sie erhalten jedoch nicht die zusätzliche Sicherheit durch die frühe Integritätsüberprüfung der Startda-

tei. Stattdessen wird die Identität des Benutzers beim Starten mithilfe eines USB-Flashlaufwerks überprüft.

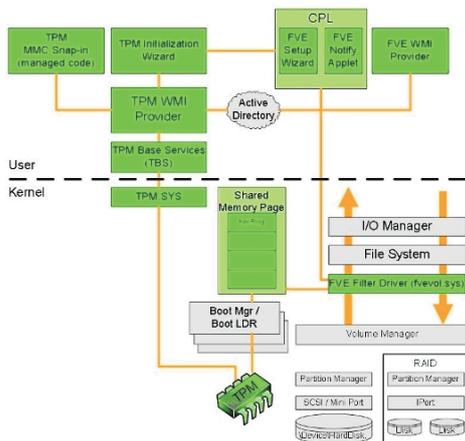
BitLocker verfügt über zwei TPM-Modi:

- **TPM-only (Nur TPM):** Dieser Modus ist für den Benutzer transparent, und die Benutzeranmeldung erfolgt unverändert. Wenn das TPM jedoch fehlt oder geändert wird, startet BitLocker den Wiederherstellungsmodus, und Sie benötigen einen Wiederherstellungsschlüssel oder ein Wiederherstellungskennwort, um wieder auf die Daten zugreifen zu können.

- **Startup key (Systemstartschlüssel):** Der Benutzer benötigt einen Systemstartschlüssel, um sich am Computer anzumelden. Ein Systemstartschlüssel kann ein physischer (ein USB-Flashlaufwerk, auf das ein computerlesbarer Schlüssel geschrieben wurde) oder ein persönlicher (eine vom Benutzer festgelegte PIN) Schlüssel sein.

Außerdem unterstützt BitLocker einen Modus für Systeme ohne TPM:

- **USB Flash Drive key (Schlüssel auf einem USB-Flashlaufwerk):** Der Benutzer schließt vor dem Einschalten ein USB-Flashlaufwerk an den Computer an. Der Computer wird mit dem auf dem Flashlaufwerk gespeicherten Schlüssel entspert.



### Gesicherte Daten: BitLocker arbeitet mit dem TPM zusammen und schützt so die Daten zuverlässig. (Quelle: Microsoft)

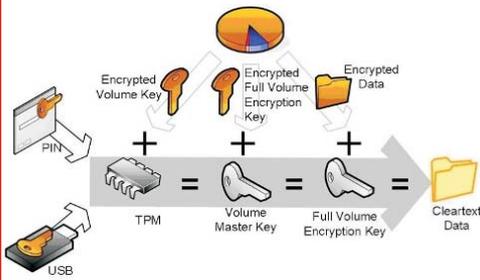
BitLocker verwendet bevorzugt Systeme, die ein **Trusted Platform Module Version 1.2 (TPM 1.2)** aufweisen. Der notwendige Chip ist aktuell nur in einzelnen Business-Systemen verbaut, soll aber Bestandteil der kommenden Sicherheitsarchitekturen Presidio (AMD) und LaGrande (Intel) sein.

BitLocker schützt Festplatten sogar nach ihrem aktiven Einsatz. Wenn der Lebenszyklus einer Platte beendet ist, musste sie bisher entweder mechanisch verschrottet oder aufwendig gelöscht werden, um wirklich alle darauf enthaltenen Daten zu beseitigen. Nun reicht es, die entsprechenden Schlüssel zu löschen. Selbst wenn jemand die Festplatten in einen anderen PC einbaut, bleiben die Daten ohne die passenden Zugangsdaten unlesbar.

Die BitLocker-Technologie setzt an zwei Punkten an. Zum einen führt sie bei jedem Bootvorgang eine Integritätsprüfung durch, zum anderen verschlüsselt sie die ausgewählten Festplattenpartitionen.

http://www.microsoft.com/windows/windows-7/

CLUBSYSTEM.NET



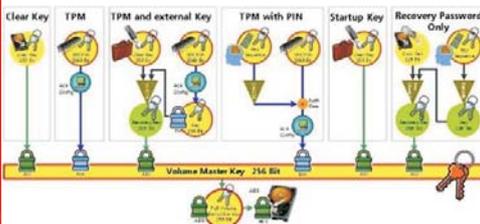
**Zutritt verweigert: Nur wenn alle digitalen Schlüssel passen, werden die Daten entschlüsselt. (Quelle: Microsoft)**

BitLocker greift dabei auf TPM zurück, um von dem System eine Art Fingerabdruck zu erzeugen. Solange an der eigentlichen Hardware nichts manipuliert wird, bleibt der digitale Fingerabdruck derselbe. Während des Bootvorgangs gleicht BitLocker die Daten ab, erst wenn die beiden Schlüssel übereinstimmen, werden die Daten auf der Festplatte entschlüsselt.

Wahlweise kann der Administrator auch einen PIN oder einen Hash-Key auf einem USB-Stick anfordern lassen, mit dem sich der Nutzer zusätzlich verifizieren muss. Erst wenn alle Schlüssel als gültig anerkannt sind, werden die Daten entschlüsselt, und der Startvorgang wird fortgesetzt.

Die Verschlüsselung der Partitionen macht sich ebenfalls TPM zu Nutze. Zunächst wird die angebene Partition mit dem *Full Volume Encryption Key (FVEK)* verschlüsselt; dieser nutzt einen 256-Bit-AES-Algorithmus. Anschließend wird der FVEK erneut verschlüsselt, diesmal mit dem *Volume Master Key (VMK)*, ebenfalls in 256 Bit AES.

Der *Volume Master Key* wird also als zusätzliche Schicht zwischen dem Anwender und den verschlüsselten Daten eingeführt. Das hat mehrere Vorteile. Der Anwender kommuniziert nie direkt mit dem Basisschlüssel, kann diesen also nicht mitloggen oder auslesen. Wenn die Sicherheit kompromittiert wurde, muss zudem nur der VMK neu erzeugt werden. Ein Ent- und anschließendes Neuverschlüsseln sämtlicher Partitionen mit geändertem Key ist daher nicht notwendig.



**Schlüsselbrett: Der Volume Master Key dient als zentraler Zugangsschlüssel. (Quelle: Microsoft)**

Aus dem VMK schließlich werden alle Schlüsselwerte für den Nutzer und die Recovery-Optionen erstellt. Löscht man also einen kompromittierten VMK, haben alle damit erstellten Schlüssel keinen Zugriff mehr.

**8.11 Vorbereiten der Laufwerkskonfiguration für den Einsatz von BitLocker**

Windows BitLocker-Laufwerkverschlüsselung ist ein Feature, das ein oder mehrere an den Computer angeschlossene Volumes (Laufwerke) verschlüsselt und die Integrität früher

Startkomponenten mit einem **TPM (Trusted Platform Module)** verifizieren kann. Da BitLocker das gesamte Datenvolumen verschlüsselt, muss der Computer mit einer aktiven, vom Betriebssystemvolumen getrennten Partition konfiguriert sein, die für den Start verwendet wird. Dies wird als Konfiguration mit aufgeteilter Last (Split-Load-Konfiguration) bezeichnet. Benutzerdaten werden entweder auf dem Betriebssystemvolumen oder zusätzlichen Datenvolumen gespeichert, die ebenfalls mit BitLocker verschlüsselt werden können.

**Voraussetzungen für die Aktivierung der BitLocker-Laufwerkverschlüsselung:**

- Mindestens zwei Partitionen (auch Volumes genannt). Eine Partition ist für das Betriebssystem vorbehalten (in der Regel Laufwerk C) und wird von BitLocker verschlüsselt, während die andere Partition die aktive Partition ist, die unverschlüsselt bleiben muss, damit der Computer gestartet werden kann. Die Größe der aktiven Partition muss mindestens 1,5 GB betragen.

- Beide Partitionen müssen mit dem NTFS-Dateisystem formatiert sein.

Ein standardmäßiges Windows 7-Setup richtet die Partitionen bereits passend ein.

Sollten Sie von Windows Vista auf Windows 7 migrieren, so können Sie die Änderungen der Konfiguration mit dem *BitLocker Drive Preparation Tool* (KB933246) durchführen, welches die nötigen Laufwerksänderungen automatisch durchführt. Konkret werden folgende Prozesse automatisiert:

1. Ein zweites Volume wird erstellt, wenn noch keines vorhanden ist.
  2. Die Startdateien werden auf das richtige Volume verschoben, und es wird sichergestellt, dass das Betriebssystem ordnungsgemäß konfiguriert ist, damit die Dateien beim Start gefunden werden.
  3. Das richtige Volume wird als aktive Partition auf dem Laufwerk für den Start konfiguriert.
- Starten Sie den Computer neu, wenn das Tool fertig ist. Das Festplattenlaufwerk des Computers wird dann ordnungsgemäß für BitLocker konfiguriert.

**8.12 Nutzung von BitLocker-Technologie ohne TPM-Chip**

Normalerweise ist für einen sinnvollen Einsatz der BitLocker-Laufwerkverschlüsselung ein TPM-Chip notwendig. Mit der MMC-Konsole *tpm.msc* kann der TPM-Chip initialisiert und verwaltet werden.

Ist kein TPM-Chip verfügbar, so erscheint in der beim Anklicken von "TPM-Verwaltung" folgende Meldung:

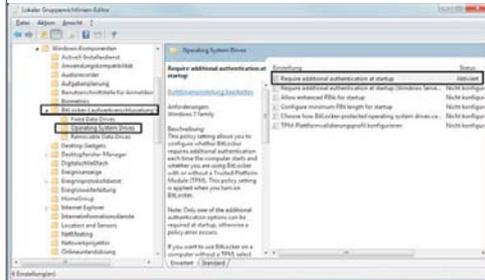


Es gibt jedoch eine Möglichkeit, BitLocker auch ohne TPM-Chip zu nutzen - die Einstel-

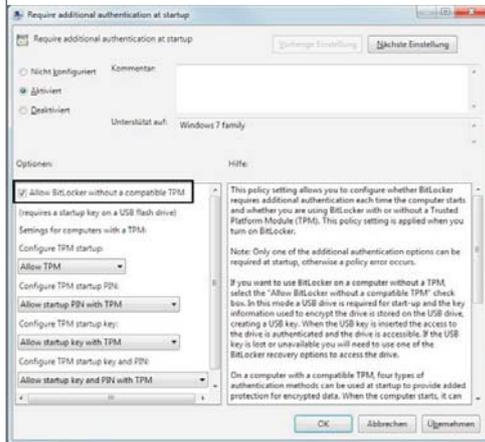
lung scheint bewusst versteckt und undokumentiert zu sein und wird auch in den FAQ von Microsoft nicht erwähnt.

Öffnen Sie den Gruppenrichtlinien-Editor (*gpedit.msc* im Startmenü eingeben)

Bearbeiten Sie auf *Computerkonfiguration - Administrative Vorlagen - Windows-Komponenten - BitLocker-Laufwerkverschlüsselung - Operating System Drives* die Richtlinie „Require additional authentication at startup“:

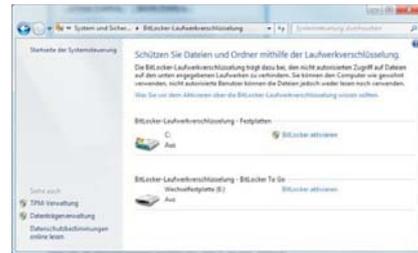


Wählen Sie nun im oberen Fensterteil "aktiviert" und setzen Sie darunter das Häkchen in "BitLocker ohne kompatibles TPM zulassen" - schließen Sie alle Fenster mit ok.



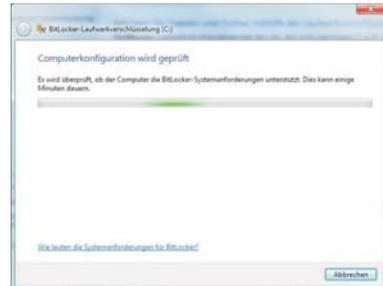
**8.13 Aktivieren von BitLocker**

Nach diesen vorbereitenden Schritten kann BitLocker aktiviert werden. Durch Anklicken der Systemsteuerungsoption „BitLocker-Laufwerkverschlüsselung“ erscheint folgende Darstellung:



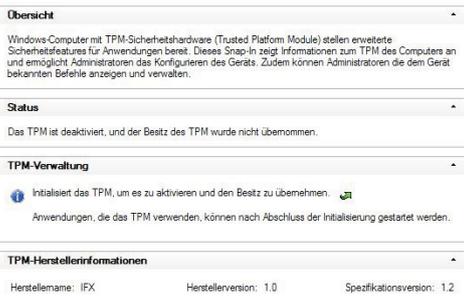
Klicken Sie auf „BitLocker aktivieren“ und folgen Sie den Anweisungen des Installations-Assistenten für BitLocker:

Wenn nun der Bitlocker-Assistent gestartet wird, zeigt er die neue Option an:



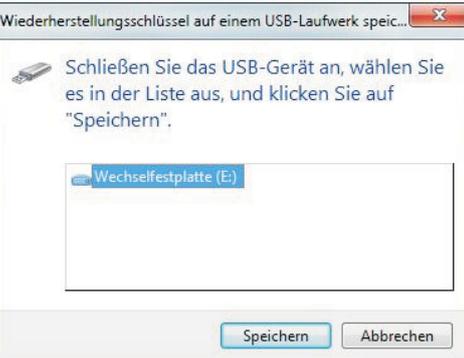
Unter „TPM-Verwaltung“ sieht man einen Überblick über den Status des TPM-Moduls.

**Beispiel:** Computer mit deaktiviertem TPM-Chip



In diesem Beispiel muss der TPM-Chip im CMOS-Setup aktiviert werden.

**Beispiel:** Computer mit aktiviertem TPM-Chip



Üblicherweise wird man einen USB-Stick verwenden, um den Schlüssel darauf zu speichern, aber auch USB-Festplatten oder Speicherkarten können hier ausgewählt werden.

Diese Lösung hat den zusätzlichen Charme, dass der USB-Stick damit quasi zum "General-schlüssel" für den Computer wird. Ist der Stick nicht eingesteckt, fährt der Rechner nicht hoch.

Ebenso fatal sind natürlich die Folgen, wenn der Stick versehentlich gelöscht wird oder einen Defekt erleidet. Man sollte die Schlüssel-daten daher doppelt und dreifach sichern, sonst kommt man im Fall des Falles nicht mehr an seine eigenen Daten.

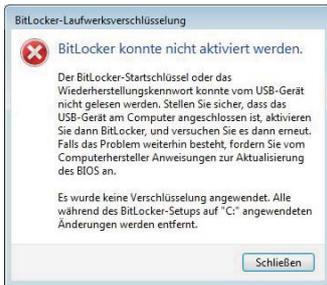


Speichert man das Wiederherstellungskenn-wort, so entstehen Dateien wie folgende:

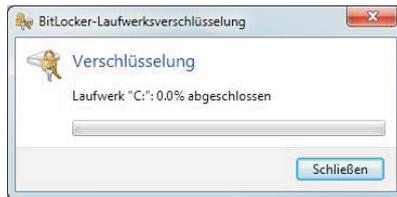


Der Dateiname ist gleichzeitig die Kenn-wort-ID.

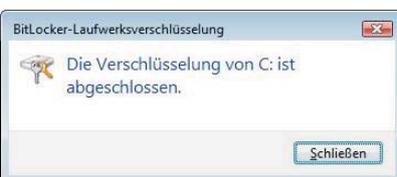
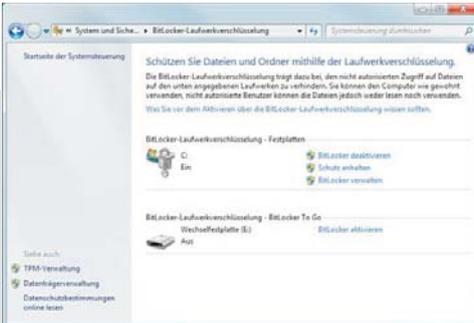
Aktiviert man die **Bitlocker-Systemüberprüfung**, so wird vor der eigentlichen Verschlüsselung ein Neustart durchgeführt und gleichzeitig versucht, vom USB-Stick das Wiederherstellungskennwort zu lesen. Gibt es dabei Probleme, so wird nicht verschlüsselt und folgende Meldung angezeigt:



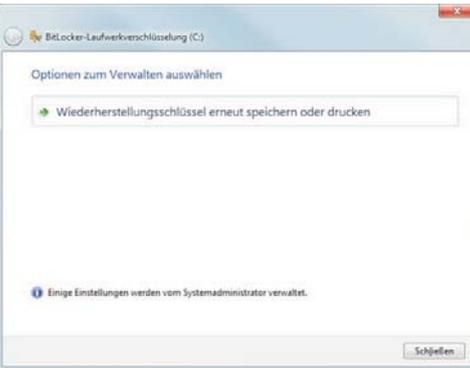
Wenn alles in Ordnung war, so wird online mit der Verschlüsselung begonnen. Ein paralleles Weiterarbeiten ist möglich, der PC reagiert aber langsamer.



Nach dem Verschlüsselungsvorgang präsentiert sich das Systemsteuerungsmenü „Bitlocker“ folgendermaßen:



Unter "Verwalten":



Startet man nun den PC ohne dem USB-Stick, so kann Windows nicht gestartet werden. Stattdessen erscheint folgende Meldung:



Es bestehen nun zwei Möglichkeiten:

- Anschließen des USB-Sticks, auf dem der Schlüssel gespeichert wurde und **[ESC]** für nochmaligen Startvorgang
- **[ENTER]** für Recovery-Modus: Hiefür wird das ausgedruckte bzw. in einer Textdatei gespeicherte Kennwort benötigt.

Dieses Kennwort mit mit Hilfe der Funktions-tasten **[F1] - [F10]** eingegeben, wie am folgenden Bildschirm erläutert wird:

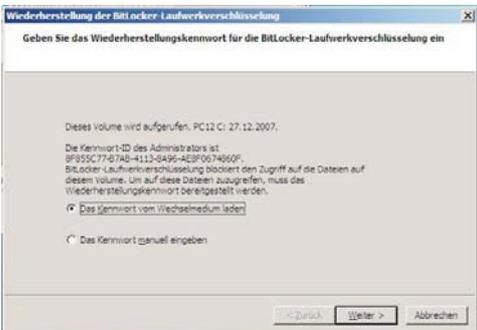


http://www.microsoft.com/windows/windows-7/

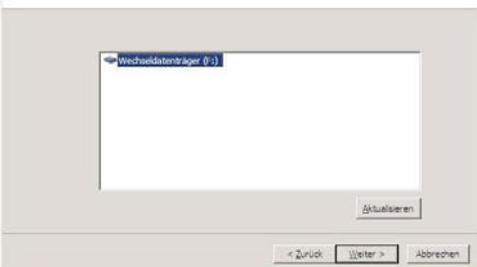
CLUBSYSTEM.NET



Versucht man, den Datenzugriff durch eine Reparaturinstallation (von Windows 7-DVD starten, Reparaturoptionen wählen), so wird ebenfalls der USB-Stick verlangt:



Legen Sie das Gerät mit dem Wiederherstellungskennwort ein und geben Sie ein Laufwerk an



Nachdem der Schlüssel vom USB-Stick geladen wurde, kommt die abschließende Meldung:



**8.14 Deaktivieren von BitLocker**

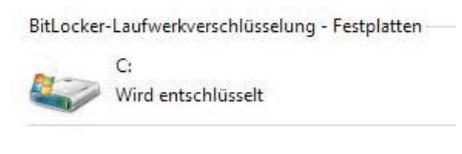
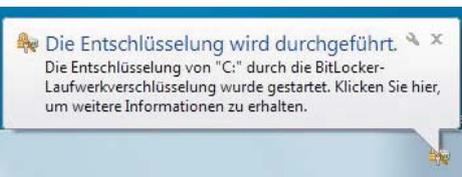
BitLocker kann auf zwei Arten deaktiviert werden: durch Anhalten von BitLocker oder durch Entschlüsseln des Laufwerks. Wenn Sie BitLocker anhalten, ist das Laufwerk immer noch verschlüsselt, aber der Computer verwendet zum Lesen der Informationen einen Nur-Text-Entschlüsselungsschlüssel, der auf dem Laufwerk gespeichert ist. Wenn Sie das Laufwerk entschlüsseln, wird der gesamte Inhalt des Laufwerks entschlüsselt.

Durch Anhalten der BitLocker-Laufwerkverschlüsselung wird der BitLocker-Schutz vorübergehend entfernt, wobei das Laufwerk, auf dem Windows installiert ist (das Betriebssystemlaufwerk), nicht entschlüsselt wird. Halten Sie BitLocker an, wenn Sie das BIOS (Basic Input/Output System) oder die Startdateien des Computers aktualisieren müssen. Diese Maßnahme hilft zu verhindern, dass BitLocker das Laufwerk sperrt, und kann einen zeitaufwändigen Entschlüsselungsprozess vermeiden. Wenn die Aktualisierung abgeschlossen ist und der Computer neu gestartet wurde, können Sie auf Schutz fortsetzen klicken.

BitLocker kann nur auf Betriebssystemlaufwerken angehalten werden. Wenn Sie BitLocker auf einem eingebauten Datenlaufwerk (z. B. einer internen Festplatte) oder einem Wechselmedien (z. B. einer externen Festplatte)

oder einem USB-Flashlaufwerk) deaktivieren möchten, müssen Sie das Laufwerk entschlüsseln.

Beim **Entschlüsseln** eines Betriebssystemlaufwerks wird der BitLocker-Schutz vom Computer entfernt. Dieser Vorgang kann sehr zeitaufwändig sein.



**8.2 BitLocker-to-Go**

**BitLocker To Go** ermöglicht die Verschlüsselung externer Medien, wie etwa USB-Sticks oder Wechselplatten.

Mit **BitLocker To Go** kann man auch wunderbar lokale Partitionen und / oder externe Festplatten schützen, aber dazu an anderer Stelle mehr. Der BitLocker unterstützt exFat, FAT 16, FAT 32 und NTFS. Die **Stärke der Verschlüsselung** ist mit 128 Bit und einer **AES-Verschlüsselung** als recht sicher zu bezeichnen. Über den *Local Group Policy Editor* kann man die Stärke der Verschlüsselung noch auf 256 Bit erhöhen sowie eine andere Art der Verschlüsselung wählen.

Ein durch BitLocker To Go verschlüsselter USB-Stick kann auf jedem Windows-Rechner, an den man ihn anschließt, benutzt werden. Nur unter Windows 7 hat man Lese- und Schreibrechte, d.h. unter **Windows XP und Windows Vista** kann man die **verschlüsselten Daten nur lesen, aber nicht speichern!**

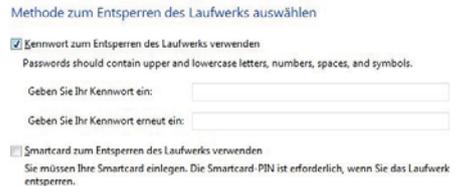
Der Zugriff auf die **verschlüsselten Dateien wird durch ein Passwort** oder eine **Smartcard** geschützt. Ein unter Windows 7 verschlüsselter USB-Stick funktioniert wie ein verschlüsselter Container, d.h. Dateien, die man hinein verschiebt sind geschützt und Dateien, die man hinaus kopiert sind nicht mehr geschützt.

**Aktivieren von BitLocker-to-Go**

Die Aktivierung erfolgt durch das Kontextmenü des Wechselmediums:



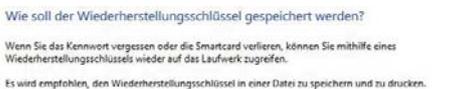
Die Art des Zugriffsschutzes wählen (Kennwort oder Smartcard)...



Im nächsten Schritt wählt man, wie der Wiederherstellungsschlüssel gespeichert werden soll.

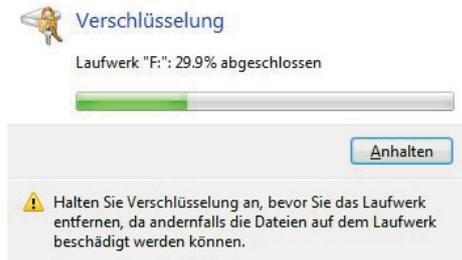
Die Datei bietet keine Sicherheit vor Hackern und der analoge Weg bietet Einbrechern die Chance Deine wertvollen verschlüsselten Daten zu entschlüsseln. Ich habe mich für digitalen Schlüssel entschieden, weil ich noch weite Schlüssel dieser Art habe.

Wichtig! Der Wiederherstellungsschlüssel ist zur Wiederherstellung der Daten, wenn man das Kennwort vergessen hat. Die BitLocker-Verschlüsselung knacken dürfte nicht leicht werden, so dass ich empfehle den Wiederherstellungsschlüssel gut aufzubewahren!



- ➔ Wiederherstellungsschlüssel in Datei speichern
- ➔ Wiederherstellungsschlüssel drucken

Im nächsten Schritt wird der Stick verschlüsselt. Das USB-Stick verschlüsseln dauert einige Zeit je nach Größe.



Im Explorer erscheint der verschlüsselte USB-Stick mit einem Schloss-Symbol:



Über das Kontextmenü kann man den BitLocker USB-Stick verwalten. Die letzte Option ist kritisch zu betrachten, da bei "automatischer Entsperrung" der Schutz nicht gegeben ist.

Optionen zum Verwalten auswählen

- ➔ Kennwort zum Entsperren des Laufwerks ändern
- ➔ Kennwort vom Laufwerk entfernen
- ➔ Smartcard zum Entsperren des Laufwerks hinzufügen
- ➔ Wiederherstellungsschlüssel erneut speichern oder drucken
- ➔ Laufwerk auf diesem Computer automatisch entsperren

Ein verschlüsselter USB-Stick, der an einen Windows-Rechner gesteckt wird, meldet sich per Autostart mit dieser Meldung:



Solange das Passwort nicht eingegeben wurde sieht man den Stick mit einem Schloss versehen und ein Anklicken des Laufwerk führt wieder zur Abfrage des Kennwortes.



Unter Windows XP oder Windows Vista, den sog. Legacy-Systemen, startet man für die Nutzung des USB-Sticks das **BitLocker to Go Lese-tool**. Das Lesetool gewährt, wie erwähnt und wie der Name es sagt, nur den Lesezugriff auf die Dateien und auch nur über die Oberfläche selbst und nicht über den Explorer.



**Verschlüsselung bzw. BitLocker entfernen**

Die einfachste Möglichkeit, die BitLocker-Verschlüsselung zu entfernen ist die Neuformatierung des USB-Sticks – dadurch gehen aber alle Daten verloren.

Der bessere Weg ist über *Systemsteuerung > System und Sicherheit > BitLocker Laufwerkverschlüsselung*.



**8.3 Windows-Tool zum Entfernen bössartiger Software**

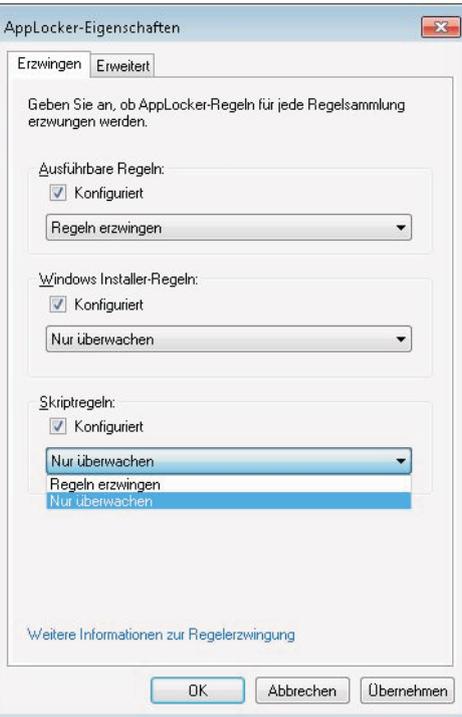
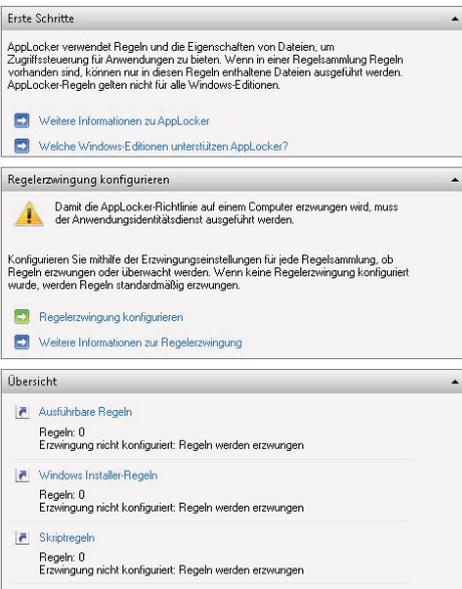
Und das Windows-Tool zum Entfernen bössartiger Software durchsucht Ihren PC regelmäßig auf bekannte weit verbreitete Viren. (Dieses Tool ist keine Komponente von Windows 7, sondern kann gratis von der Microsoft-Webseite heruntergeladen werden.)

**8.4 AppLocker**

Seit Windows XP gibt es Gruppenrichtlinien für Softwareeinschränkungen. Diese Richtlinien waren bisher sehr schwierig bzw. aufwändig zu konfigurieren, da sie auf dem Hash-Wert von ausführbaren Programmdateien beruhen.

Das AppLocker-Konzept versteht sich als einfacher zu konfigurierende Alternative. AppLocker-Einstellungen können entweder als lokale Richtlinie unter Windows 7 oder als Gruppenrichtlinie unter Windows Server 2008 R2 eingerichtet werden:

- ➔ Sicherheitseinstellungen
  - ➔ Kontorichtlinien
  - ➔ Lokale Richtlinien
    - ➔ Überwachungsrichtlinie
    - ➔ Zuweisen von Benutzerrechten
    - ➔ Sicherheitsoptionen
    - ➔ Windows-Firewall mit erweiterter Sicherheit
    - ➔ Netzwerklisten-Manager-Richtlinien
    - ➔ Richtlinien für öffentliche Schlüssel
    - ➔ Richtlinien für Softwareeinschränkung
    - ➔ Anwendungssteuerungsrichtlinien
    - ➔ AppLocker



**9 Kompatibilität**

**9.1 WindowsXP-Mode**

Der Windows XP-Mode beruht auf einer lizenzfreien Installation von Windows XP SP3 als virtuelle Maschine innerhalb von Windows 7.

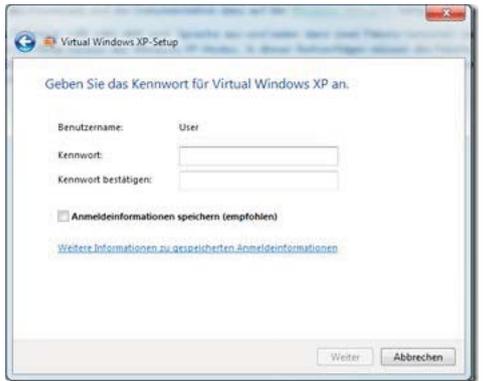
Download: <http://www.microsoft.com/windows/virtual-pc/default.aspx>

Zunächst wählen Sie Ihre Windows 7-Version (x86 oder x64) und -Sprache aus und laden dann zwei Pakete herunter: Die Beta-Version von Windows Virtual PC 7 und die Beta-Version des Windows XP-Modus. In dieser Reihenfolge müssen die Pakete auch installiert werden; nach der ersten Installation ist zusätzlich ein Neustart notwendig. Achtung: Für eine erfolgreiche Installation von Windows Virtual PC muss das PC-BIOS Hardware-Virtualisierung unterstützen (z.B. Intel-VT, AMD-V)!

Windows Virtual PC 7 weist eine Reihe interessanter Features auf, einschließlich:

- **Seamless-Anwendungen:** Starten Sie die auf einem virtuellen Computer installierten Anwendungen direkt vom Windows 7-Desktop, so als ob sie auf dem Windows 7-Hostcomputer installiert wären.
- **Vereinfachte Benutzeroberfläche:** Verbesserte Benutzeroberfläche, die einfach zu verwenden ist. In Windows 7 Explorer integriert.
- **Integrationsfeatures:** Ermöglicht das Freigeben von Zwischenablage und Laufwerken und die Umleitung von Druckern für Windows 7 und den virtuellen Computer.
- **USB-Unterstützung:** Die Benutzer können direkt aus virtuellen Computern auf an den Hostcomputer angeschlossene USB-Geräte zugreifen. Diese Geräte schließen Drucker und Scanner, Flashmemory/Memory Sticks und externe Festplattenlaufwerke, Digitalkameras und weitere ein.

Beim erstmaligen Start des Windows XP-Modus wird die virtuelle XP-Maschine konfiguriert. Zunächst müssen Sie dem Lizenzvertrag zustimmen, danach können Sie das Paßwort für den Benutzer 'User' in der XP-Installation festlegen:



Nun kommt noch die Abfrage zur Aktivierung von automatischen Updates, und das war's dann auch schon. Wohlgedenkt: das sind alles Einstellungen für die virtuelle XP-Maschine, nicht für den Windows 7-Host!

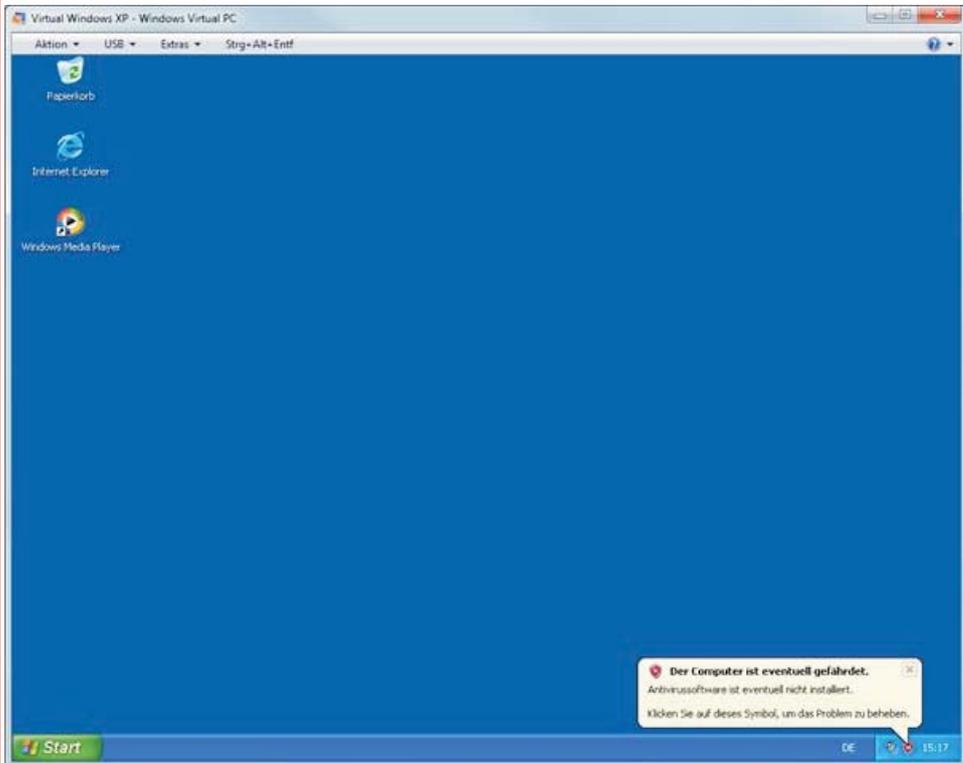
http://www.microsoft.com/windows/windows-7

CLUBSYSTEM.NET

Jetzt wird Virtual XP gestartet, was beim ersten Mal ein paar Minuten dauert, da im Hintergrund noch die XP Konfiguration fertiggestellt werden muss:

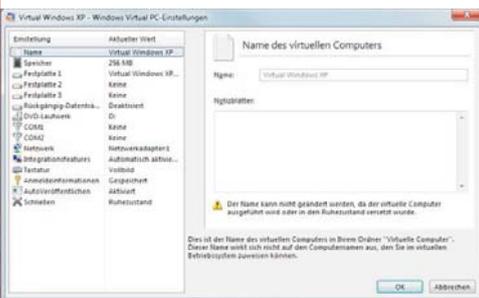


Danach hat man zunächst mal ein virtualisiertes Windows XP, wie man es z.B. von Virtual PC her gewohnt ist:



Dass man in diesem Fenster die Warnung bezüglich der nicht installierten Antivirus-Applikation sieht, weist nochmal darauf hin, dass hier wirklich ein zusätzliches Betriebssystem läuft. Firewall und Antivirus-Applikation des Windows 7-Host sind für das virtualisierte Windows XP nicht wirksam!

Einstellungen für die Virtuelle Maschine kann man im Menü unter 'Extras' - 'Einstellungen' vornehmen. Auch dieser Dialog ist aus Virtual PC bekannt. Unter 'Netzwerk' kann man hier auch eine der Host-NICs auswählen und so auf ein externes Netzwerk zugreifen. Die Einstellungen sind übrigens auch direkt im Ordner 'Virtuelle Computer' (im Benutzer-Profil) verfügbar, und zwar mit einem Rechts-Klick auf die entsprechende Virtuelle Maschine.



Besonders interessant dürfte für viele der Menüpunkt 'USB' sein. Die dort aufgeführten Geräte sind innerhalb der Virtuellen Maschine verfügbar, sobald man auf 'Anfügen' klickt. Es können z.B. Webcams, USB-Laufwerke, MP3-Player, Drucker, Smartphones und PDAs umge-

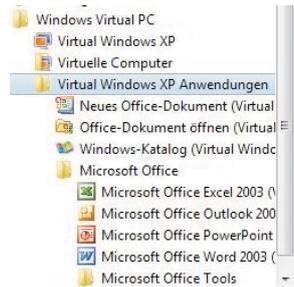
leitet werden. Drucken können Sie natürlich auch auf einen Netzwerk-Drucker.



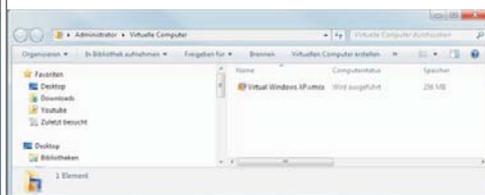
Applikationen, die man im Virtual Windows

sprechenden Seite. Von der im Hintergrund laufenden Virtuellen Maschine ist für den Benutzer dann nichts mehr zu sehen:

Weitere Applikationen werden im Startmenü der Windows 7-Hostmaschine im Menü „Virtual Windows XP-Anwendungen“ angezeigt.



Verwaltet werden die virtuellen Maschinen im Windows Explorer:



XP-Modus benutzen möchte, installiert man innerhalb der Virtuellen Maschine. Die startet man z.B. direkt aus dem Start-Menü – 'Windows Virtual PC' - #Virtual Windows XP'. Hat man bei der Erst-Konfiguration das Speicher des Passworts angegeben, wird die Anmeldung in der Virtuellen Maschine automatisch durchgeführt.

Jetzt installiert man entweder vom Netzwerk, von einer ISO-Datei oder vom Host-CD/DVD-Laufwerk (letztere kann man in den Einstellungen der Virtuellen Maschine im Punkt 'DVD-Laufwerk' verbinden). Die Applikationen tauchen dann automatisch im Start-Menü des Windows 7-Host auf (Start-Menü – 'Windows Virtual PC' – Virtual Windows XP-Anwendungen).

Vorinstalliert ist hier als Beispielanwendung der 'Windows Katalog'. Startet man die Applikation, so erscheint auf dem Windows 7-Desktop ein Internet Explorer 6-Fenster mit der ent-



Quelle: Dieser Abschnitt basiert auf einem Blog-Eintrag von Ralf M. Schnell unter <http://blogs.technet.com/sieben/>.

Für größere Umgebungen eignet sich der XP Mode nicht – die Verwaltung wäre viel zu aufwändig. Für diesen Zweck gibt es im Microsoft Desktop Optimization Pack das Paket Microsoft Enterprise Desktop Virtualization (MED-V). MED-V bietet eine Management Console für den Client-VPC, um die Images zentral verwalten, warten und kontrollieren zu können.

# Microsoft® Enterprise Desktop Virtualization