Nr. **109**/Juni 2008 € 5,00

ISSN 1022-1611

PCNEWS

ClubPocketPC ClubDigitalHome ClubSystem ClubDev ClubEducation

Windows Vista

- Neuerungen
- Drucker
- Startvorgang
- Datenträger
- Notfall
- Sicherheit
- Mobile Geräte
- Fehleranalyse

Anhang

- Kommandozeile
- PowerShell

¡hasta la vista!

covergrafiX: w.krause@chello.at

Verlagspostamt 1100 Wien, P.b.b. GZ 02Z031324 M

Inhalt

Liebe Leserinnen und Leser!

Franz Fiala, Werner Krause

PCNEWS-109

¡hasta la vista!, Auf Wiedersehen

...denn das ist unsere vorläufig letzte Folge des Vistakurses. Sie finden auf **Seite 4** ein Verzeichnis alles bisher erschienenen Vista-Artikel. **Christian Haberl** beschreibt auf **Seite 25** 18 Schritte zur exakten Fehleranalyse und **Christian Zahler** zeigt auf **Seite 6** im letzten Teil eines Vista-Kurses:

- ***Windows-Vista Neuerungen*** (Live-Symbole, Linkfavoriten, User Account Control, Security Principals, Fernanmeldung)
- ***Drucker*** (Ablauf des Druckvorgangs, lokales Druckerobjekt, TCP/IP-Drucker, Druckserver, Druckeinstellungen, Druckerpool, Erweiterte Druckereigenschaften, NTFS-Berechtigungen
- ***Startvorgang, Datenträgerverwaltung und Notfallwiederherstellung*** (Startvorgang, Backup und Restore, Notfallwiederherstellung, Systemeigenschaften, Treiber und Hardware-Installation, Tools zur Verwaltung von Festplatten, RAID)
- ***Windows Vista-Sicherheitseinstellungen*** (Sicherheitscenter, Windows Update, Windows Firewall, Windows Defender, Popup-Blocker, BitLocker, Internet-Optionen
- ***Vista und mobile Geräte***

Anhang

Für Liebhaber der Kommandozeile gibt es zu dieser Ausgabe einen Anhang, der in der Online-Version downgeloadet werden kann.

- ***Windows Kommandozeile*** (Zusammenfassung aller internen und externen Befehle aus verschiedenen Quellen; insgesamt 349 Befehle, inklusive neue Befehle für Server 2008)
- ***Windows PowerShell*** (Links auf Materialien vom gleichnamigen Clubabend von **Wolfgang Aigner** über die neue, leistungsfähige Commandline für Power-User)
- ***Video-Schnitt*** (Vortrag vom gleichnamigen Clubabend von **Oliver Hunger**)

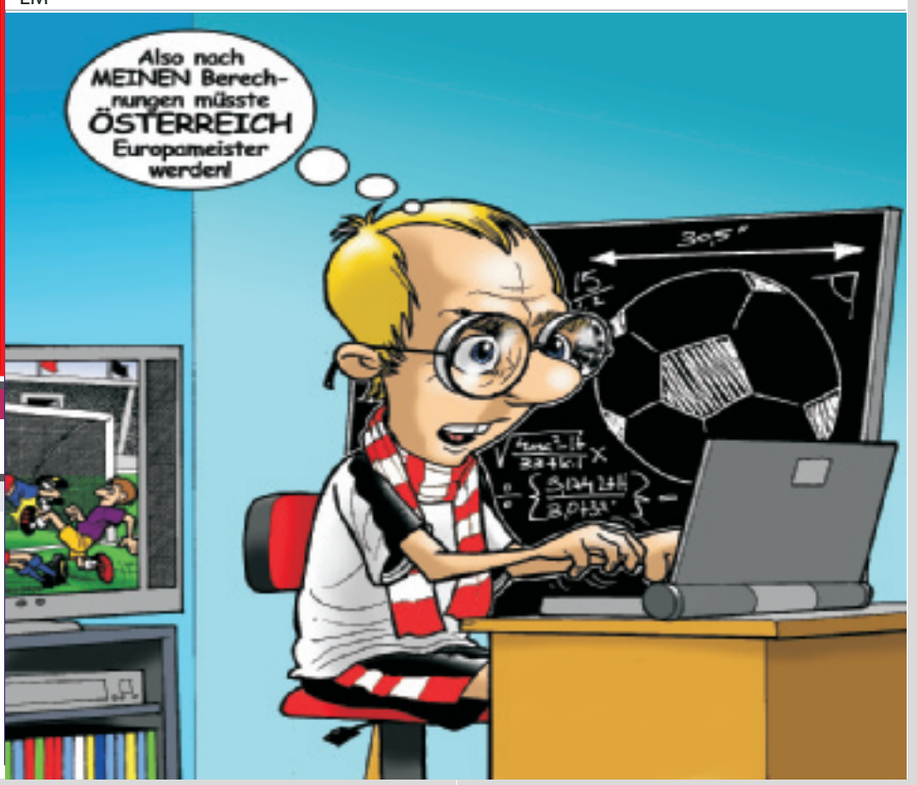
PCNEWS-110, -111 (Vorschau)

Für die Herbstausgaben der **PCNEWS** ist der Beginn von zwei neuen Kursen von **Christian Zahler** geplant:

- Windows Server 2008
- SQL-Server 2005

Franz Fiala Werner Krause

EM



www.intec.fh-burgenland.at

Internettechnologien „Zukunftsorientierte Technologien“

Fachhochschul Studiengänge

Burgenland

Bildung im Herzen Europas.

Die Anforderungen für zukünftige IT-Spezialisten werden immer höher. Zunehmende Internationalität, notwendige soziale Kompetenz und betriebswirtschaftliches Know-how sind notwendig, um im Arbeitsmarkt erfolgreich zu sein. Genau dieses Wissen wird im Bachelorstudiengang Internettechnologien vermittelt.

Im Fokus des Studiums stehen Technologien für das Internet von morgen. Die Ausbildung kombiniert Software-Entwicklung für Internet-Anwendungen, Netzsicherheit und Systemadministration sowie Webdesign und Multimedia mit dem Erwerb von Managementkompetenzen und Fremdsprachen. Interessante Praxisprojekte werden durch die Einbettung in den Informations- und Kommunikationstechnologie Cluster Burgenland ermöglicht.

Details zum Studium und Online-Anmeldung

www.intec.fh-burgenland.at

Fachhochschul-Bachelorstudiengang „Internettechnologien“

Campus 1
A-7000 Eisenstadt
Tel.: +43 (0)5 9010 603-0
Fax: +43 (0)5 9010 603-11
E-mail: office.intec@fh-burgenland.at

Autoren

Aigner Wolfgang Dipl.-Ing. 1966 A1

PMA zertifizierter Projektmanager (Level D)
Firma NTx
Absolvent TU-Graz, HTL-Linz
Hobbies Segeln, Golf, Literatur, Philosophie
E✉ *wolfgang.aigner@ntx.at*
🌐 *http://www.ntx.at/*

Berger Christian 2

Karikaturist und Comiczeichner für verschiedene Kärntner Zeitungen
Firma Karicartoons
E✉ *karicartoons@aon.at*
🌐 *http://www.bergercartoons.com/*

Fiala Franz Dipl.-Ing. 1948 2, A2

Leitung der Redaktion und des Verlags der PCNEWS, Obmann des PCC; Lehrer für Nachrichtentechnik und Elektronik i.R.
Schule TGM-N
Werdegang BFPZ-Arsenal
Club CCC MCCA PCC VIT
Absolvent TU-Wien, Nachrichtentechnik
Privates verheiratet, 1 Kind
E✉ *franz.fiala@clubcomputer.at*
🌐 *http://fiala.cc/*

Haberl Christian 1979 25

EDV-Consultant, freiberuflicher Vortragender und Trainer für Microsoft Österreich (Themen: Windows, Office, Internet, IT-Sicherheit), Direktor ClubDigitalHome
Club CCC
Hobbies Familie, Musik, Reisen, Kochen
Privates verheiratet, ein Kind
E✉ *c.haberl@this.at*
🌐 *http://www.this.at/*

Hunger Oliver A1

Firma think a Bit x-media communications
Club PCC
Absolvent HGLA/TGM-Kolleg Multimedia
E✉ *pcc@thinkabit.net*
🌐 *http://www.thinkabit.net/*

Krause Werner Mag. 1955 1,2

Lehrer für Bildnerische Erziehung
Schule GRG 23 Alterlaa, Bundesgymnasium Wien 23
Absolvent Hochschule f. Angewandte Kunst, Gebrauchsgrafik
Hobbies Fotografieren, Computergrafik (CorelDraw Photoshop u.a.) Videoschnitt, Coverbilder für PCNEWS
Privates 2 Kinder
E✉ *w.krause@chello.at*

Wagner Oskar Anton M.Sc.PhD EdD 5

Nach 38 Jahren Telekommunikation, davon 34 Jahre im Unterrichtswesen.
E✉ *wago@aon.at*
🌐 *http://members.aon.at/oe1-100470/*

Zahler Christian Mag. 1968 6

Gewerbetreibender, Autor von ADIM-Skripten, Erwachsenenbildung, Lektor für Informatik, MCSE
Firma WIFI St.Pölten, FHS Steyr
Club ADIM PCC
E✉ *office@zahler.at*
🌐 *http://www.zahler.at/*

Inserenten

●FH Burgenland 3

✉ Campus 1 7000 Eisenstadt
☺ Christiane Kerbl
☎ +43-5-9010 601-25 **FAX:** 9010 609-15
E✉ *christiane.kerbl@fh-burgenland.at*
🌐 *http://www.fh-burgenland.at/*

●MTM-Systeme 31

✉ Hadrawagasse 36 1220 Wien
☺ Ing. Gerhard Muttenthaler
☎ 01-2032814 **FAX:** 2021303
✆ 0664-4305636
E✉ *g.muttenthaler@mtm.at*
🌐 *http://www.mtm.at/*
Produkte uC/uP-Entwicklungswerkzeuge, Starterkits, Industriecomputer, Netzqualitätsanalyzer, USV-Anlagen
Vertretung Tasking, PLS, Infineon, TQ-Components, Kontron, Dranetz-BMI, Panasonic, Dr. Haag, HT-Italia, Dr. Kaneff
Erreichbar U1-Kagran, 26A bis Englisch-Feld-Gasse

●STADLER EDV-Dienstleistungs- und Handels-ges.m.b.H 32

✉ Welschgasse 3/1/7 1230 Wien
☺ Erich Stadler
☎ 01-8653990 **FAX:** 8653990-123
E✉ *office@systemsoftware.at*
🌐 *http://www.systemsoftware.at/*

Vista - PCNEWS

PCN	S.	Titel	Autor
109	9	Windows Vista Kurs-3	Christian Zahler
109	25	Fehleranalyse in Windows (Vista)	Christian Haberl
109	A1	Windows PowerShell	Wolfgang Aigner
109	6	Windows Vista Neuerungen	Christian Zahler
109	9	Windows Vista - Inhalt	Christian Zahler
109	A2	Vista Kommandozeile	Franz Fiala
108	13	Windows Vista Kurs - 2	Christian Zahler
107	7	Vista Kommandozeile von der Instal-lations-CD	Christian Haberl
107	12	Windows Vista Kurs - 1	Christian Zahler
107	31	Vista Informationen	Christian Haberl
107	A1	BDD2007	Christian Zahler
107	A3	Windows Vista Installationsverfah-ren	Christian Zahler
106	20	Die ersten Wohnzimmer PCs mit Windows Vista sind gelandet!	Christian Haberl
104	8	Windows Vista - Tastenkürzel	Christian Haberl
104	25	Windows Vista - Gadgets	Christian Haberl
103	8	Windows Vista	Christian Haberl
103	13	Windows Vista Sicherheit	Werner Illsinger

Impressum

Impressum, Offenlegung

Richtung Auf Anwendungen im Unterricht bezogene Informationen über Personal Computer Systeme. Berichte über Veranstaltungen der Herausgeber.
Erscheint 5 mal pro Jahr, Feb, Apr, Jun, Sep, Nov
Verleger PCNEWS-Eigenverlag
Siccardsburggasse 4/1/22 1100 Wien
☎01-6009933-210 **FAX:** -9210
E✉*pcnews@pcnews.at*
🌐 *http://www.pcnews.at/*
Herausgeber ClubComputer
Fernkorngasse 17/1/6 1100 Wien
☎01-6009933-11 **FAX:** -12
E✉*office@clubcomputer.at*
🌐 *http://www.clubcomputer.at/*
Druck, Versand Friedrich VDV
Zamenhofstraße 43-45, 4020 Linz
☎0732-669627-0 **FAX:** 669627-5
E✉*office@friedrichvdv.com*
🌐 *http://www.friedrichvdv.com/*

ClubComputer

Leitung, CCC Werner Illsinger
☎01-6009933-220 **FAX:** -9220
E✉*werner.illsinger@clubcomputer.at*
PCNEWS, PCC Franz Fiala
☎01-6009933-210 **FAX:** -9210
E✉*franz.fiala@clubcomputer.at*
Marketing Ferdinand De Cassan
☎01-6009933-230 **FAX:** -9230
E✉*ferdinand.de.cassan@clubcomputer.at*
ClubPocketPC Paul Belcl
☎01-6009933-288 **FAX:** -9288
E✉*paul.belcl@clubcomputer.at*
ClubDigitalHome Christian Haberl
☎01-6009933-240 **FAX:** -9240
E✉*christian.haberl@clubcomputer.at*
cc|Akademie Georg Tsamis
☎01-6009933-250 **FAX:** -9250
E✉*georg.tsamis@clubcomputer.at*

PCNEWS-109

Kennzeichnung ISSN 1022-1611, GZ 02Z031324 M
Layout Corel-Ventura 10, Corel-Draw 12.0
Herstellung Bogenoffset, 80g
Erscheint Wien, Juni 2008
Texte http://pcnews.at/?id=PCN109
Kopien Für den Unterricht oder andere nicht-kommerzielle Nutzung frei kopierbar. Für gewerbliche Weiterverwendung liegen die Nutzungsrechte beim jeweiligen Autor. (Gilt auch für alle am PCNEWS-Server zugänglichen Daten.)
Werbung A4: 1 Seite 522,- EURO U2,3,4 782,- EUR0
Beilage: bis 50g 138,- EUR pro 1000 Stück
Bezug 1 Heft: 5,- EURO (zuzüglich Versand)
5 Hefte: 20,- EURO (1 Jahr, inklusive Versand)
kostenlos für Mitglieder von ClubComputer
Hinweise Druckfehler und Irrtümer vorbehalten.
Preisangaben in Inseraten sind wegen des Fertigungszeitraums der PCNEWS von einem Monat möglicherweise nicht am letzten Stand. Wir bitten die Leser, die aktuellen Preise nachzufragen.
Alle erwähnten Produktnamen sind eingetragene Warenzeichen der entsprechenden Erzeuger.

Internet-Zugang

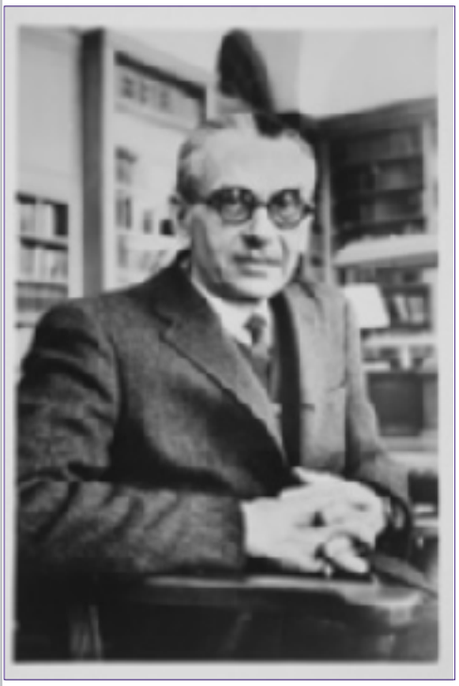
Einwahl ☎**Online-Tarif:** 0804-002222 (56k/V90 und ISDN))
Support ☎**Hotline:** 01-6009933-200
E-✉**Support:***support@ccc.at*
Konfig **Mail:** POP3: pop3.ccc.or.at SMTP: smtp.ccc.or.at
DNS: automatisch
Gateway: Standard-Gateway

Kurt Friedrich Gödel zum 30. Todestag

Wahr-Unwahr – Unentscheidbar

In jedem sinnvollen mathematischen System gibt es unentscheidbare Sätze. Gödel ist einer der berühmtesten österreichischen Mathematiker und einer bedeutendsten Logiker. Die Harvard University verlieh ihm das Ehrendoktorat für die Entdeckung „der bedeutsamsten mathematischen Wahrheit des Jahrhunderts". Das Time Magazine reihte ihn unter die hundert wichtigsten Personen des zwanzigsten Jahrhunderts.

Oskar Wagner



Kurt Friedrich Gödel wurde am 28. April 1906 in Brünn, der Hauptstadt des österreichischen Kronlandes Mähren, die damals eine deutschsprachige Bevölkerungsmehrheit hatte, geboren. Er entstammt wohlhabendem Großbürgertum. Sein Vater Rudolf kam aus Wien war ein Textilunternehmer und katholisch, seine Mutter Marianne kam aus dem Rheinland und war evangelisch. Sein älterer Bruder Rudolf wurde 1902 geboren. In seiner Kindheit litt Kurt Gödel oft unter rheumatischem Fieber, erbrachte aber trotz seines schlechten Gesundheitszustandes schulische Höchstleistungen. Nach der Volksschule besuchte er das deutschsprachige k. k. Staatsrealgymnasium. Nach dem Ersten Weltkrieg wurde die Stadt Brünn Teil der neu gegründeten Tschechoslowakischen Republik. Da er die tschechische Sprache kaum beherrschte, fühlte er sich in dem neu gegründeten Staat nicht heimisch und, nach eigenen Worten, wie ein *„österreichischer Verbannter in Tschechoslowakien".*

1923 nahm er deshalb die österreichische Staatsbürgerschaft an, zog im Herbst 1924 nach Wien und begann theoretische Physik zu studieren. Er beschäftigte sich hauptsächlich mit physikalischen Themen, besuchte aber auch die philosophische Vorlesung von Heinrich Gomperz[1] sowie die Vorlesung über die Zahlentheorie von Philipp Furtwängler[2]. Diese Beiden gaben Gödel die entscheidenden Impulse, sich intensiv mit jenen Grundlagen der Mathematik auseinanderzusetzen, welche auf der formalen Logik sowie der Mengenlehre beruhen. Kurz nach Beginn seiner Studien begann er den Wiener Kreis[3] zu besuchen, wo er sich mit den methodischen Grundlagen des Denkens und somit den Grundlagen jedweder Philosophie auseinandersetzte. Am 6. Februar 1930 promovierte er zum Dr.phil. In seiner Habilitationsschrift von 1931 - *Über formal unentscheidbare Sätze der Principia Matematica und verwandter Systeme* - sind die beiden Unvollständigkeitssätze enthalten, die die mathematische Welt erschütterten und deren Grenzen aufzeigte.

Mit seinen Unvollständigkeitssätzen bewies Gödel, dass es in einem System wie der Arithmetik, das auf unmittelbar einleuchtenden Ausgangssätzen (Axiomen) beruht, immer Aussagen gibt, die weder bewiesen noch widerlegt werden können. Das erschütterte den Glauben an die Mathematik als das „absolut Sichere". Wahrheit und Beweisbarkeit sind nicht mehr identisch.

1938 heiratete Kurt Gödel Adele Porkert, die er zu diesem Zeitpunkt schon über 10 Jahre kannte. Nach dem Anschluss Österreichs an das Deutsche Reich verlor Gödel wegen der Umstellung des Bildungssystems seine österreichische Dozentur und versuchte zunächst eine adäquate akademische Stelle im nunmehr deutschen Bildungssystem zu erhalten. Die entsprechenden Anträge wurden jedoch sehr schleppend bearbeitet, weshalb er sich entschloss - obwohl nicht rassisch verfolgt - in die USA auszuwandern.

Nach seiner Einreise in die USA und dem Beginn seiner Arbeit am *„Institute for Advanced Study"* in Princeton, New Jersey, begann sich Gödel immer mehr mit philosophischen Problemen zu beschäftigen und sich von der formalen Logik abzuwenden. 1942 lernte er Albert Einstein näher kennen und begann mit ihm über physikalische Probleme wie die Relativitätstheorie oder über philosophische Themen zu diskutieren. Zwischen Einstein und Gödel entwickelte sich eine enge Freundschaft, die bis zu Einsteins Tod 1955 anhielt. Nach eigener Aussage ging Einstein in späteren Jahren nur deshalb ans Institut, um Gödel auf dem Heimweg begleiten zu dürfen. Gödel gab die erste Lösung der Allgemeinen Relativitätstheorie mit geschlossenen zeitartigen Weltlinien an, die zeigt, dass „Zeitreisen" rein theoretisch möglich wären. In einer Randbemerkung hält Gödel fest, dass die Zeitrichtung bei der Landung des Reisenden wieder dieselbe ist, also nicht verkehrt abläuft wie in einem falsch eingelegten Film.

In den 1940-er und 1950-er Jahren vereinsamte Gödel, der 1948 die amerikanische Staatsbürgerschaft angenommen hatte, aufgrund seiner fortschreitenden psychischen Krankheit immer mehr. Er hatte panische Angst, durch Speisen vergiftet zu werden. In den sechziger Jahren hörte er auf, Vorlesungen zu geben und seine Krankheit ließ ihm immer weniger die Möglichkeit zu arbeiten.

Er galt aber weiterhin als einer der führenden Logiker und seine akademischen Leistungen wurden mit verschiedenen Auszeichnungen und mehreren Ehrendoktoraten amerikanischer Universitäten gewürdigt. Sein Gesundheitszustand besserte sich allerdings nicht. 1970 versuchte er zum letzten Mal zu publizieren. Die Schrift musste jedoch zurückgenommen werden, da er aufgrund der Wirkung von Psychopharmaka viele Fehler einfach übersehen hatte.

Seine letzten Lebensjahre verbrachte Gödel zu Hause in Princeton bzw. in verschiedenen Sanatorien, aus denen er einige Male flüchtete. Lediglich der Fürsorge seiner Frau ist es zu verdanken, dass er sich wenigstens halbwegs normal ernährte. Als Adele Gödel selbst einen Schlaganfall erlitt und an einen Rollstuhl gefesselt war, musste sie hilflos zusehen, wie ihr Mann immer mehr abmagerte. Am 14. Jänner 1978 verstarb Kurt Gödel bei einem Körpergewicht von 40 kg an Unterernährung und Entkräftung.

Fußnoten

1. Heinrich Gomperz, geb. 18. Jänner 1873 in Wien, verst. 27. Dezember 1942 in Los Angeles, Philosoph
2. Philipp Furtwängler, geb. 21. April 1869 in Elze, verst. 19. Mai 1940 in Wien, deutscher Mathematiker der vor allem auf dem Gebiet der Zahlentheorie tätig war
3. Der Wiener Kreis war eine Gruppe von Philosophen und Wissenschaftstheoretikern, die sich von 1922 bis 1936 wöchentlich in Wien trafen

Links

Biografie

http://de.wikipedia.org/wiki/Kurt_G%C3%B6del/

Vollständigkeitssatz

http://de.wikipedia.org/wiki/G%C3%B6delscher_Vollst%C3%A4ndigkeitssatz/

Unvollständigkeitssatz

http://de.wikipedia.org/wiki/G%C3%B6delscher_Unvollst%C3%A4ndigkeitssatz

Vista Neuerungen

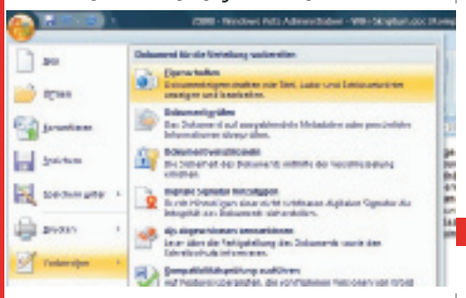
Christian Zahler

Live-Symbole

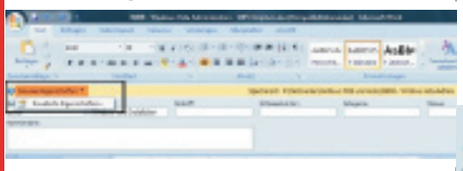
Über die neue Live-Symbol-Funktion können Sie Dateien schneller finden und ihren Inhalt erkennen, ohne sie öffnen zu müssen.

Die Hauptelemente der Explorer unter Windows Vista sind so gestaltet, dass Sie die benötigen Informationen zum gewünschten Zeitpunkt finden. Die Schnellsuche steht stets bereit, damit Sie Dateien unmittelbar finden können. Der Navigationsbereich enthält die neue Windows Vista-Suchordnerfunktion sowie herkömmliche Ordner, die Sie auf dem Computer erstellt haben. Auf Befehlsleisten werden nur die Aufgaben angezeigt, die für die angezeigten Dateien am geeignetsten sind. Mit Hilfe der neuen Live-Symbole (skalierbare Miniaturansichten) in Windows Vista können Sie die erste Seite von Dokumenten, den Inhalt eines Fotos oder das "Cover" einzelner Songs in Ihrer Musiksammlung anzeigen, sodass Sie das gesuchte Element einfacher finden können.

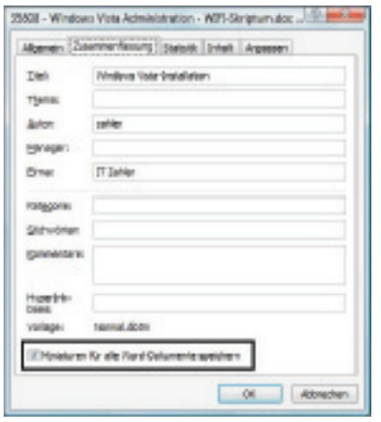
Voraussetzung für die Verfügbarkeit der Live-Symbole ist, dass beim Abspeichern einer Datei ein Abbild der ersten Seite erstellt wird. Dieses Abbild wird in der versteckten Datei `Thumbnails.db` hinterlegt. Dies kann bei Office 2007 folgendermaßen erreicht werden: Klicken Sie auf die Office-Schaltfläche und wählen *[Vorbereiten]* – *[Eigenschaften]*:



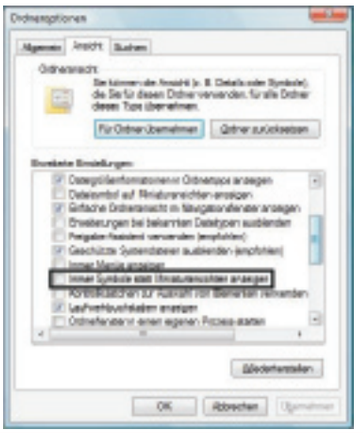
In der nun eingeblendeten Eigenschaftsleiste wählen Sie aus dem Menü *[Dokumenteigenschaften]* – *[Erweiterte Eigenschaften]*:



Im nun eingeblendeten Dialogfeld wählen Sie die Karteikarte *„Zusammenfassung"* und überprüfen, ob am unteren Rand dieser Karteikarte der Eintrag *„Miniaturen für alle Word-Dokumente speichern"* aktiviert ist.



Die Miniaturansichten werden allerdings nur angezeigt, wenn der Ordneroptions-Eintrag *„Immer Symbole statt Miniaturansichten anzeigen"* deaktiviert ist.



Linkfavoriten im Explorer definieren

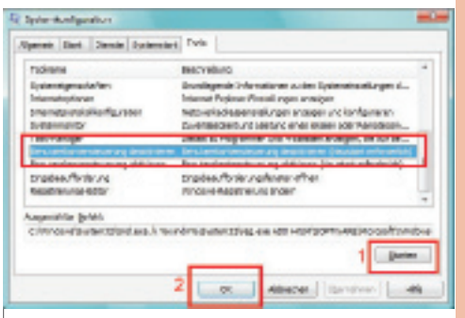
Navigieren Sie in der Ordnerstruktur zu einem gewünschten Ordner. Ziehen Sie dann das Ordnersymbol in der Adresszeile in den Linkfavoriten-Bereich, so wird der Ordner zu den Linkfavoriten hinzugefügt. Damit lässt sich der Zugriff auf Ordner mit langen Pfadangaben, die häufig benötigt werden, massiv beschleunigen.

Abschalten der User Account Control

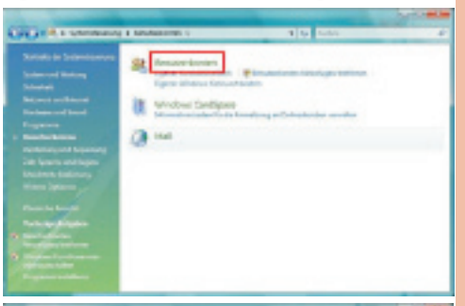
Es wird darauf hingewiesen, dass das Abschalten der UAC ausdrücklich nicht empfohlen wird!

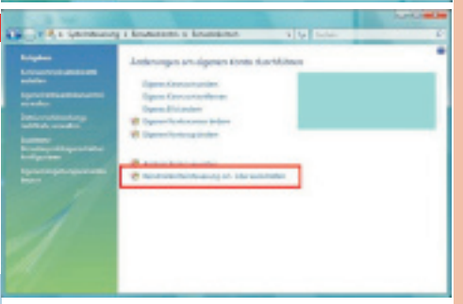
Die UAC kann auf zwei Arten abgeschaltet werden:

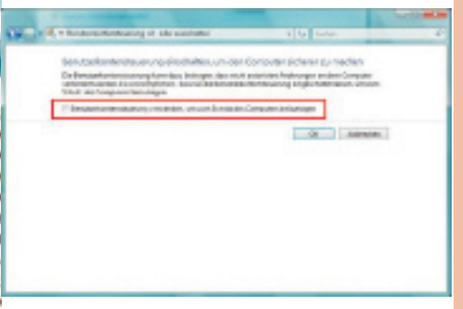
Methode 1: Mittels *Ausführen* (*Start* -> *Ausführen* -> `msconfig` (alternativ Windows-Taste R -> `msconfig`) dem Ablauf *Tools* -> *Benutzerkontensteuerung deaktivieren* -> *Starten* folgen



Methode 2: Wählen Sie den Systemsteuerungs-Menüpunkt *„Benutzerkonten"* (*Systemsteuerung – Benutzerkonten – Benutzerkonten – Benutzerkontensteuerung ein- oder ausschalten*) und deaktivieren Sie die Einstellung *Benutzerkontensteuerung verwenden*, um zum Schutz des Computers beizutragen. Anschließend mit *OK* bestätigen.



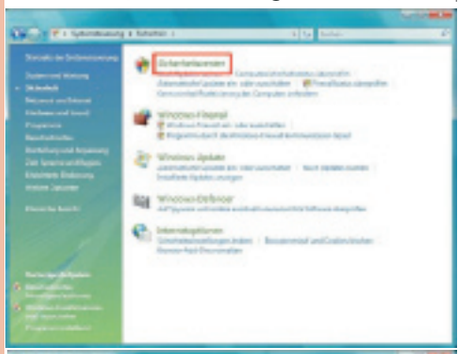


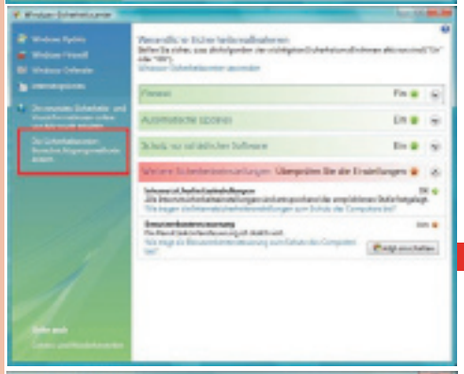


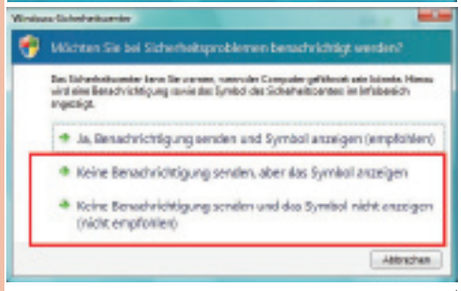
Sicherheitswarnung abschalten

Jedoch hat dies einen kleinen Nachteil: Es erscheint fortwährend eine Sicherheitswarnung, dass die Benutzerkontensteuerung deaktiviert sei. Möchte man nicht oder nicht direkt darauf hingewiesen werden, so kann man diese (und andere Meldungen des Sicherheitscenters) deaktivieren. Hierzu ist folgendes zu tun:

Im Sicherheitscenter (Systemsteuerung – Sicherheit – Sicherheitscenter) im Linken Bereich auf Die Sicherheitscenter-Benachrichtigungsmethode ändern klicken. Im darauf folgenden Fenster wahlweise auf Keine Benachrichtigung senden, aber das Symbol anzeigen oder auf Keine Benachrichtigung senden und das Symbol nicht anzeigen (nicht empfohlen) auswählen (Ablauf siehe folgende Bilder)







Abschalten der UAC nur für die Administratoren-Gruppe (Registry-Einstellung):

Ein weiterer Weg, die Benutzerkontensteuerung zu beeinflussen, ist, diese nur für die Benutzer der Gruppe *Administratoren* zu deaktivieren.

Hierfür muss man sich dem Registry-Editor zu Hilfe nehmen (*Start* -> *Ausführen* -> `registry(regedit)`)

Hier gibt es im Pfad

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`

einen Eintrag `ConsentPromptBehaviorAdmin` vom Typ `REG_DWORD`. Dieser muss ggf. noch angelegt werden. Dieser kann folgende Werte annehmen:

0 Keine Aufforderungen mehr seitens der Benutzerkontensteuerung - alle Programme werden mit höheren Rechten ausgeführt
1 Bestätigung für höhere Rechte erforderlich. Weiterhin muss das Kennwort des Benutzers eingegeben werden.
2 Einfache Zustimmung über die Anforderung von höheren Rechten. Ein Kennwort ist nicht erforderlich (**Standard-Einstellung**)

Achtung: Aus Sicherheitsgründen sollte auch für die Administrator-Gruppe davon abgesehen werden, die Benutzerkontensteuerung auszuschalten.

Abschalten der UAC nur für die Standard-Benutzer-Gruppe (Registry-Einstellung)

Wenn die Benutzerkontensteuerung nur für Standard-Benutzer eingestellt werden, benötigt man den Registry-Editor.

Hier gibt es einen Eintrag `ConsentPromptBehaviorUser` (ggf. muss dieser noch angelegt werden) im Pfad

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`

Dieser ist vom Typ `REG_DWORD` und kann die folgenden Werte annehmen:

0 Keine Aufforderungen mehr seitens der Benutzerkontensteuerung - sollte jedoch ein Programm erhöhte Rechte benötigen, so werden diese **verweigert** und das Programm könnte eventuell nicht mehr oder nicht richtig ausgeführt werden.
1 Bestätigung für höhere Rechte erforderlich. Weiterhin muss das Konto eines Administrators mit dessen Kennwort eingegeben werden (**Standard-Einstellung**).

Achtung: Aus Sicherheitsgründen sollte davon abgesehen werden, die Benutzerkontensteuerung zu beeinflussen.

Security Principals

Unter diesem Begriff werden Objekte zusammengefasst, denen Berechtigungen zugewiesen werden können.

Zu den wichtigsten *Security Principals* zählen:

- Benutzerkonten
- Computerkonten
- Gruppenkonten

Benutzer-, Computer- und Gruppenkonten werden nicht über ihren Namen, sondern über einen internen Primärschlüssel, den sogenannten *Security Identifier (SID)*, verwaltet. Alle Berechtigungen für Benutzer-, Computer- und Gruppenkonten werden intern mit dieser SID gespeichert.

Aufbau einer SID

- **Domänen-SID**: Im Fall von lokalen Benutzerkonten spezifiziert diese Nummer den PC, bei Domänen-Benutzerkonten die Domäne. Alle lokalen Benutzerkonten auf demselben PC haben dieselbe Domänen-SID; alle AD-Benutzer derselben Domäne haben ebenfalls dieselbe Domänen-SID.
- **RID (Relative ID)**: Diese oft vierstellige Nummer ist spezifisch für jedes Benutzer-, Computer- oder Gruppenkonto. Dabei hat das vordefinierte Administrator-Konto immer die RID 500. So hätte das Administrator-Konto des obigen PCs folgende SID:

`S-1-5-21-1812011286-570857186-3424489074-500`

SIDs können beispielsweise mit dem Tool `PsGetSID` angezeigt werden (Download unter *http://www.microsoft.com/technet/sysinternals/utilities/psgetsid.mspx*).

Well-Known SIDs

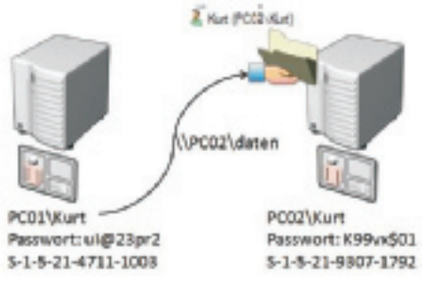
Einige *Security Principals* haben SIDs, die nicht wie oben beschrieben aufgebaut sind. Es handelt sich dabei um **Spezialidentitäten**, die vom System her vorgesehen sind und sich in vielen Fällen ähnlich wie Gruppenkonten verhalten. Die wichtigste Gemeinsamkeit dieser speziellen Objekte ist die immer gleiche SID – egal auf welchem PC oder in welcher Domäne. Die Mitgliedschaft wird vom Betriebssystem gesteuert und kann nicht geändert werden.

Beispiele (siehe nächste Seite):

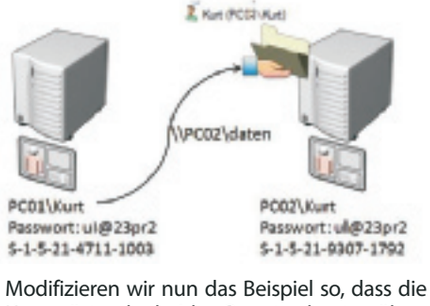
Fernanmeldung, automatische Fernanmeldung

Beispiel: Wir nehmen an, dass auf einem Rechner mit dem Namen `PC02` ein freigegebener Ordner mit dem Freigabenamen `daten` existiert. Auf beiden Rechnern wurde ein lokaler Benutzer mit dem Anmeldenamen `Kurt` erzeugt. Die beiden Benutzer haben unterschiedliche Kennwörter und natürlich auch unterschiedliche SIDs.

Die Sicherheitsberechtigungen für den Ordner `daten` wurden so eingerichtet, dass nur der Benutzer `Kurt` Zugriffsrechte (zum Beispiel *„Ändern“*) auf diesen Ordner hat.



Wir nehmen nun an, dass sich `PC01\Kurt` mit dem UNC-Pfad `\\PC02\daten` zum freigebenen Ordner verbinden will. Die LSA *(Local Security Authority)* auf `PC02` überprüft Benutzername, Kennwort und SID. Nur eine von diesen drei Eigenschaften stimmt überein (der Benutzername), daher wird `PC01\Kurt` nicht ohne weiteres der Zugriff auf den Ordner gewährt; es erscheint ein **Dialogfeld für die Fernanmeldung**:



Modifizieren wir nun das Beispiel so, dass die Kennwörter der beiden Benutzerkonten übereinstimmen. Wieder überprüft die LSA auf `PC02` Benutzername, Kennwort und SID – zwei dieser drei Eigenschaften stimmen überein (Benutzername und Kennwort). Nun erscheint kein Dialogfeld; es erfolgt eine automatische Fernanmeldung. Die Zugriffsberechtigungen für `PC01\Kurt` sind so, als hätte er sich als `PC02\Kurs` angemeldet.

Beispiele für SIDs

SID	Name	Beschreibung
S-1-1-0	*Everyone (Jeder)*	Gruppe, die alle Benutzer einschließlich der anonymen Benutzer und Gäste enthält. Die Mitgliedschaft wird vom Betriebssystem gesteuert. Hinweis: Seit Windows XP Service Pack 2 (SP2) sind anonyme Benutzer standardmäßig nicht mehr Mitglied der Gruppe *"Everyone"*.
S-1-3-0	*Ersteller-Besitzer*	Platzhalter in einem vererbbaren ACE-Eintrag. Wenn der ACE-Eintrag geerbt wird, ersetzt das System diesen SID durch den SID des Objekterstellers.
S-1-5-1	*Dialup (DFÜ)*	Gruppe, die alle Benutzer enthält, die sich über eine DFÜ-Verbindung angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-2	*Netzwerk*	Gruppe, die alle Benutzer enthält, die sich über eine Netzwerkverbindung angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-3	*Batch (Batch)*	Gruppe, die alle Benutzer enthält, die sich über eine Batch-Warteschlangeneinrichtung angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-4	*Interactive (Interaktiv)*	Gruppe, die alle Benutzer enthält, die sich interaktiv angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-6	*Service (Dienst)*	Gruppe, die alle Sicherheitsprinzipale enthält, die sich als Dienst angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-7	*Anonymous (Anonym)*	Gruppe, die alle Benutzer enthält, die sich anonym angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-9	*Enterprise Domain Controllers (Domänencontroller der Organisation)*	Gruppe, die alle Domänencontroller in einer Gesamtstruktur enthält, die einen Verzeichnisdienst des Active Directory verwenden. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-10	*Principal Self (Selbstprinzipal)*	Platzhalter in einem vererbbaren ACE-Eintrag für ein Konto- oder Gruppenobjekt im Active Directory. Wenn der ACE-Eintrag geerbt wird, ersetzt das System diesen SID durch den SID des Sicherheitsprinzipals, dem das Konto gehört.
S-1-5-11	*Authenticated Users (Authentifizierte Benutzer)*	Gruppe, die alle Benutzer enthält, deren Identitäten bei der Anmeldung authentifiziert wurden. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-13	*Terminal Server Users (Terminalserverbenutzer)*	Gruppe, die alle Benutzer enthält, die sich bei einem Terminaldiensteserver angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-18	*Lokales System*	Dienstkonto, das vom Betriebssystem genutzt wird.
S-1-5-19	*NT Authority (NT-Autorität)*	Lokaler Dienst
S-1-5-20	*NT-Autorität*	Netzwerkdienst
S-1-5-32-544	*Administratoren*	Vordefinierte Gruppe. Nach der Erstinstallation des Betriebssystems ist das Administratorkonto einziges Mitglied der Gruppe. Wenn ein Computer einer Domäne beitritt, wird die Gruppe *"Domänen-Admins"* der Administratorengruppe hinzugefügt. Wenn ein Server zum Domänencontroller wird, wird die Gruppe *"Organisations-Admins"* ebenfalls zur Administratorengruppe hinzugefügt.
S-1-5-32-545	*Benutzer*	Vordefinierte Gruppe. Nach der Erstinstallation des Betriebssystems ist die Gruppe der authentifizierten Benutzer einziges Mitglied dieser Gruppe. Wenn ein Computer einer Domäne beitritt, wird die Gruppe der Domänenbenutzer zur Benutzergruppe auf dem Computer hinzugefügt.
S-1-5-32-546	*Gäste*	Vordefinierte Gruppe. Standardmäßig ist das Gastkonto einziges Mitglied dieser Gruppe. Die Gästegruppe ermöglicht es Gelegenheitsbenutzern oder einmaligen Benutzern, sich mit eingeschränkten Berechtigungen über das vordefinierte Gastkonto auf einem Computer anzumelden.
S-1-5-32-547	*Hauptbenutzer*	Vordefinierte Gruppe. Standardmäßig hat diese Gruppe keine Mitglieder. Hauptbenutzer können lokale Benutzer und Gruppen erstellen, von ihnen selbst erstellte Konten ändern und löschen und Benutzer aus den Hauptbenutzer-, Benutzer- und Gästegruppen löschen. Hauptbesucher können außerdem Programme installieren, lokale Drucker erstellen, verwalten und löschen sowie Dateifreigaben erstellen und löschen.

Windows Vista

Christian Zahler

Drucker

Man unterscheidet grundsätzlich:

- **Physischer Drucker**
- **Logisches Druckerobjekt**

Unter einem **physischen Drucker** versteht man die eigentliche Hardware. Einem **physischen Drucker** können mehrere logische Druckerobjekte (mit unterschiedlichen Treibern und Konfigurationseinstellungen) zugeordnet werden; umgekehrt kann ein logisches Druckerobjekt mit mehreren physischen Druckern gleicher Bauart verknüpft werden („Druckerpool").

Unter einem **logischen Druckobjekt** versteht man die Kombination eines Druckertreibers (Software) mit bestimmten Konfigurationseinstellungen. Um also von Windows aus drucken zu können, muss ein **logisches Druckerobjekt** eingerichtet werden. Dabei unterscheidet man grundsätzlich:

- **Lokale Drucker(objekte)**
- **Netzwerkdrucker(objekte)**

Lokale Druckerobjekte werden lokal erstellt. Sie werden in der lokalen Registrierdatenbank (Registry) des jeweiligen Rechners gespeichert.

Lokale Druckerobjekte müssen mit einem Treiber und Anschlussinformationen hinterlegt werden.

Es ist nicht zwingend nötig, dass der Drucker physisch mit dem PC verbunden ist; so gelten auch Drucker mit eingebauter oder externer Netzwerkkarte (umgangssprachlich auch als „Printserver" bezeichnet) als lokale Drucker.

Arten von Anschlüssen:

- Parallel (LPT1)
- Seriell (COM1)
- USB
- Netzwerkkarten mit IP-Adresse

Netzwerkdruckerobjekte verweisen zu freigegebenen lokalen Druckerobjekten, die auf einem anderen PC erstellt wurden.

Netzwerkdruckerobjekte müssen mit einem UNC-Pfad zur entsprechenden Freigabe hinterlegt werden, zum Beispiel
`\\server02\HPLaserJet`.

Ablauf des Druckvorgangs

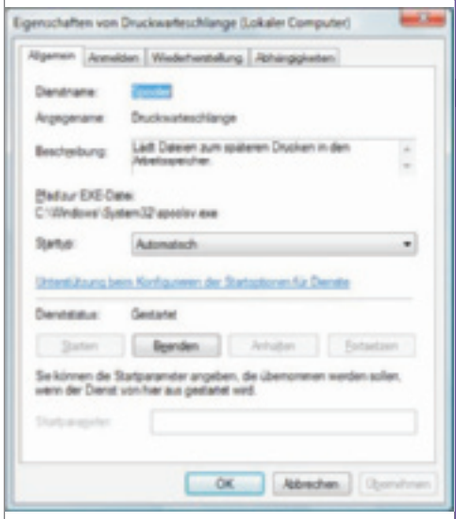
Wird ein Druckvorgang durchgeführt, so laufen dabei folgende Schritte ab:

1. Je nach installiertem Drucker wird eine Druckdatei erstellt. Diese Druckdatei kann zum Beispiel in den Druckersprachen PCL *(Printer Control Language)*, PS *(PostScript)* oder HOPGL *(Hewlett Packard Graphics Language)* geschrieben sein. Es handelt sich dabei immer um eine Textdatei, die Anweisungen an den jeweiligen Drucker enthält.

Ausschnitt einer PostScript-Druckdatei:

```
F /F0 0 /256 T /Helvetica mF
/F0S53 F0 [83 0 0 -83 0 0 ] mFS
F0S53 Ji
473 550 M (Dieser Text soll gedruckt
werden.)[60 18 46 42 46 28 23 52 46 42 23 23 42
46 18 18 24 46 46 46 29 46 42 43 23 23 59 46 28
46 46 46
 0]xS
1708 550 M ( )S
473 646 M ( )S
LH
(%%[Page: 1]%%) =
%%PageTrailer
```

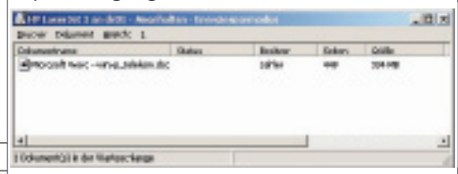
2. Diese Druckdatei wird an den **Druckspooler** *(Spool = Simultaneous Peripheral Operation On-Line)* weitergeleitet. Es handelt sich dabei um einen lokal operierenden Dienst, der Druckaufträge (englisch: Jobs) in Druckwarteschlangen (englisch: Queues) verwaltet.



Die Druckwarteschlangen können lokal vorhanden sein – oder, im Fall eines Druckservers – auch auf anderen Rechnern.

Wichtig: Für die Druckaufträge muss ausreichend Platz auf der Festplatte vorhanden sein (Druckaufträge können mehrere 100 MB groß werden, siehe Abbildung!).

In der Druckwarteschlangenverwaltung können Druckaufträge gelöscht werden, der Drucker „angehalten" werden (das bedeutet, der Spool-Vorgang wird unterbrochen).



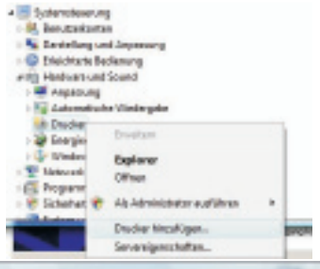
3. Die Druckdateien werden dann an den angegebenen Drucker weitergeleitet. Dabei kann der Drucker immer nur so viele Daten empfangen, wie er in seinem Arbeitsspeicher unterbringen kann.

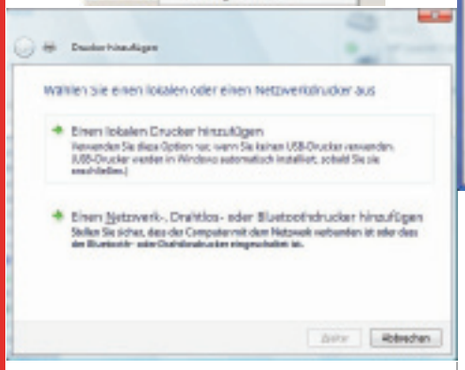
4. Der Drucker arbeitet die in seinem Arbeitsspeicher befindlichen Druckaufträge seitenweise (Laserdrucker) bzw. zeilenweise (Nadel-, Tintenstrahldrucker) ab. Nicht benötigte Druckinformationen werden gelöscht, sodass im RAM Platz für weitere Teile des Druckauftrags bzw. neue Druckaufträge geschaffen wird.

Inhaltsverzeichnis

Einrichten eines lokalen Druckerobjekts

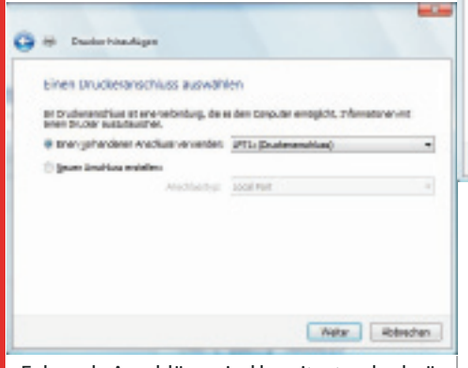
Über die Systemsteuerung im Objekt *„Drucker und Faxgeräte“* auf *„Drucker hinzufügen“* klicken. Es startet folgender Assistent:





1. Schritt: Geben Sie im Assistenten an, dass ein lokales Druckerobjekt erstellt werden soll. Wenn der Drucker tatsächlich physisch an den PC **angeschlossen und eingeschaltet** (!) ist, kann das Kontrollkästchen *„Plug & Play-Drucker automatisch ermitteln und installieren“* aktiviert bleiben.

2. Schritt: Wählen Sie den **Druckeranschluss** aus oder erstellen Sie einen neuen Anschluss.

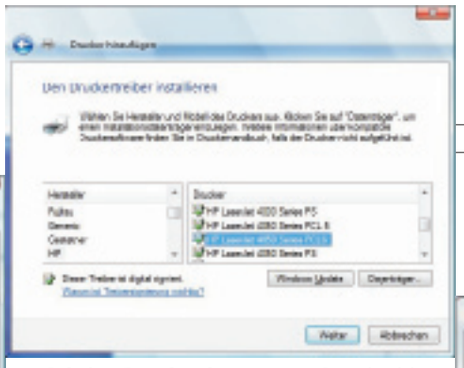


Folgende Anschlüsse sind bereits standardmäßig vorhanden:

- **Parallele Anschlüsse (LPT1, …)**: Früher der Standard-Druckeranschluss; erforderlich ist ein paralleles Kabel mit Centronics-Stecker.
- **Serielle Anschlüsse (COM1, …)**: Wurde häufig für CAD-Plotter verwendet. Voraussetzung für das Funktionieren des Druckers ist die übereinstimmende Konfiguration der seriellen Schnittstellen auf PC und Drucker (zum Beispiel Übertragungsrate – 9600 bps).
- **Umleitung in Datei (FILE:):** Die Druckdaten werden nicht an den Druckspooler gesendet, sondern in eine Druckdatei geschrieben (Dateierweiterung *.prn). Der Ausdruck selbst kann dann später bzw. auf einem nicht lokal vorhandenen Drucker erfolgen.
- **Microsoft Document Imaging Writer Port (Local Port):** Ist Office 2003 auf dem PC installiert, so kann mit diesem Anschluss eine `*.mdi`-Datei erzeugt werden, ein sehr platzsparendes Format, das nicht mehr bearbeitet werden kann, aber mit dem Microsoft Document Imaging-Tool betrachtet und gedruckt werden kann (ähnlich PDF).

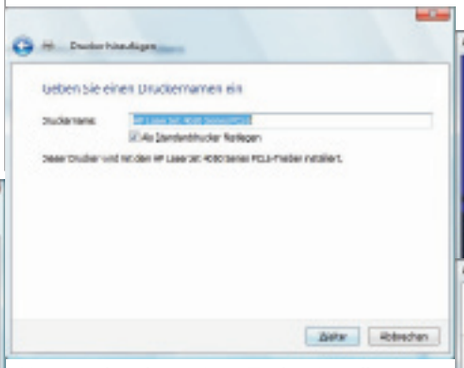
Nicht vorhanden sind TCP/IP-Anschlüsse, die gebraucht werden, wenn der Drucker über eine Netzwerkkarte verfügt, die mit dem Netzwerk verbunden ist (siehe später).

3. Schritt: Auswählen des **Druckertreibers**



4. Schritt: Drucker benennen, Standarddrucker konfigurieren

Die Konfiguration als Standarddrucker ist insofern wesentlich, als viele Softwaretools grundsätzlich auf dem Standarddrucker auswählen (zum Beispiel wird bei der Druckerauswahl im Menü *[Datei] – [Drucken]* nur der Standarddrucker geändert!).



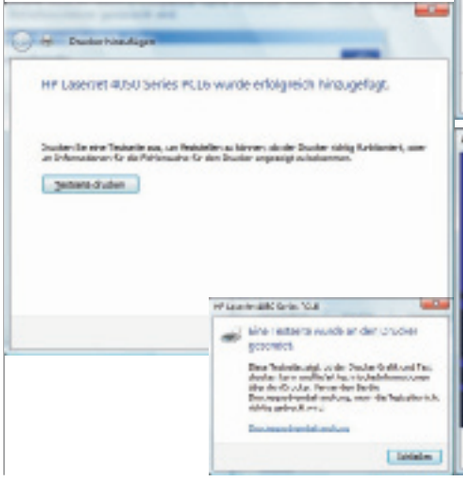
Nun werden die nötigen Treiber installiert.

5. Schritt: Testseite drucken

Eine letzte Kontrolle des eingerichteten Druckers stellt die Testseite dar, die aus

- grafischen Informationen,
- Systemschrift-Texten und
- TrueType-Schrift-Texten

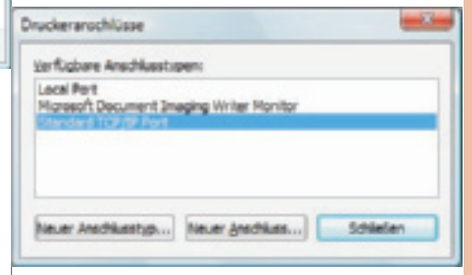
besteht. Überprüfen Sie speziell, ob diese drei Elemente korrekt dargestellt werden. Wenn nicht, sollten Sie einen anderen Druckertreiber wählen.



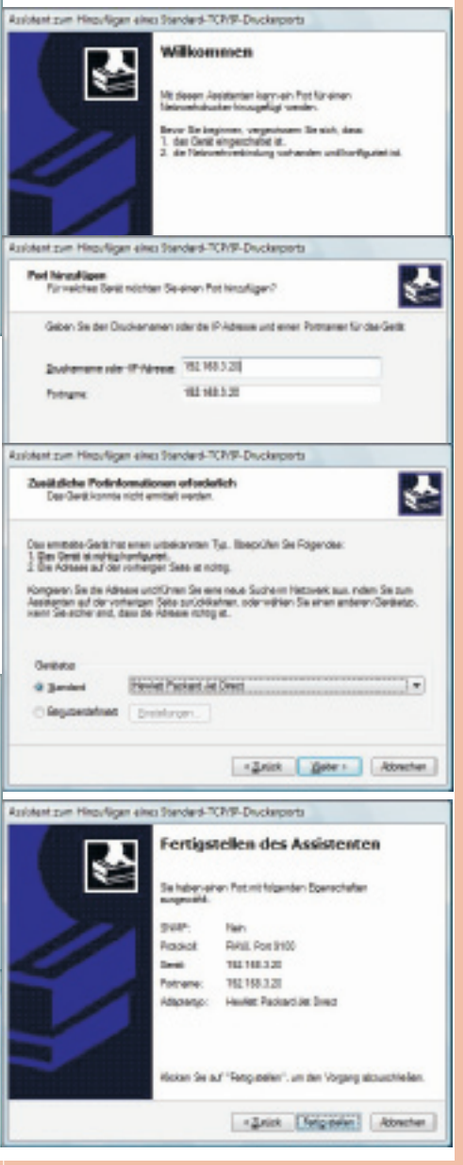
So sollte eine Drucker-Testseite aussehen:

Erzeugen eines TCP/IP-Druckeranschlusses

Dies ist notwendig, wenn der lokale Drucker über eine eigene Netzwerkkarte bzw. über eine externe Netzwerkkarte (falsch auch als „Printserver“ bezeichnet, etwas korrekter „Netport“) verfügt.



Druckserver konfigurieren:

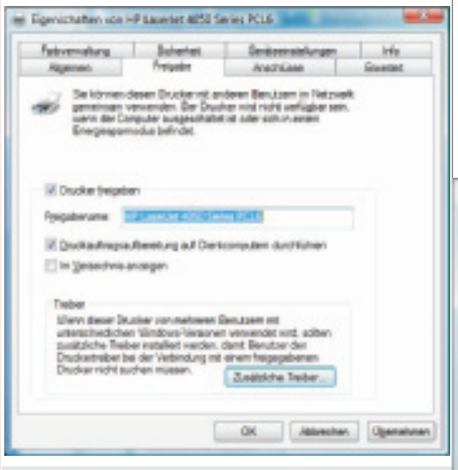


Schritt 1: Drucker freigeben

Eine Druckerfreigabe basiert auf denselben technischen Grundlagen wie Ordnerfreigaben. Als Freigabename muss ein NetBIOS-kompatibler Name verwendet werden, wenn die Integration mit älteren Betriebssystemen gewünscht wird.

Zunächst müssen die Freigabeoptionen des logischen Druckerobjekts geändert werden:

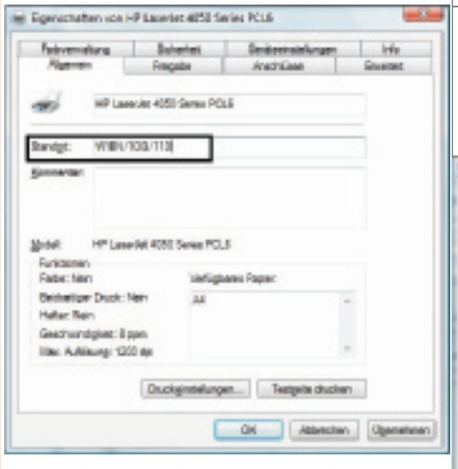
Dann muss ein Freigabename festgelegt werden:



Wichtig: Ein freigegebener Drucker wird auch als Druck-Server bezeichnet!

2. Schritt: Standortangabe und Kommentar

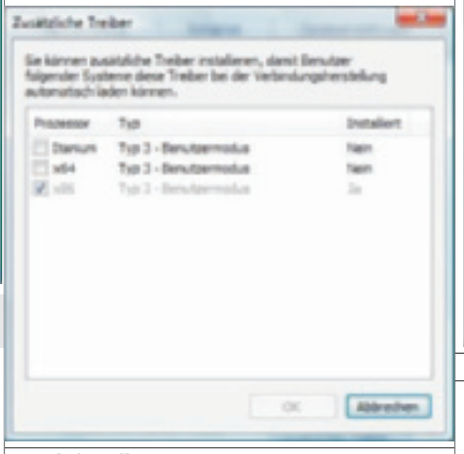
Bei der Angabe des Standorts sollten Sie eine Hierarchie berücksichtigen, mit Hilfe derer der Drucker wieder gefunden werden kann.



Wenn Sie einen Druckserver konfiguriert haben (zur Erinnerung: das ist ein freigegebener Drucker), dann haben Sie zwei weitere Möglichkeiten:

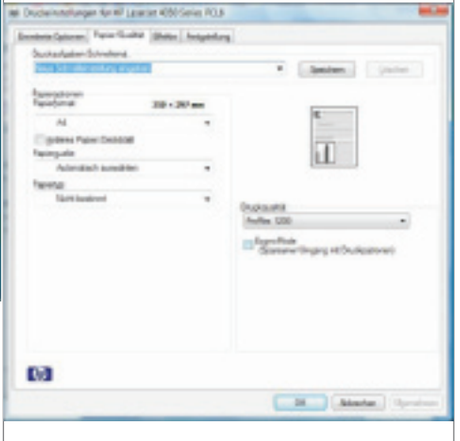
- Veröffentlichung der Druckerfreigabe im Active Directory (nur in AD-Domänen möglich): Dazu muss der Eintrag *„Im Verzeichnis anzeigen"* aktiviert werden

- Bei der Freigabe von Druckern wird automatisch eine administrative Freigabe **PRINT$** erzeugt, die zu einem Ordner führt, in welchem passende Druckertreiber vorhanden sind. Bei der Installation eines Netzwerkdruckers können Client-PCs diese Treiber herunterladen, ohne das Druckermodell kennen zu müssen. Standardmäßig werden in diese Freigabe nur Treiber für Windows 2000/XP/2003 gestellt; mit der Schaltfläche *„Zusätzliche Treiber"* können auch Treiber für ältere Windows-Plattformen in diese Freigabe gestellt werden.

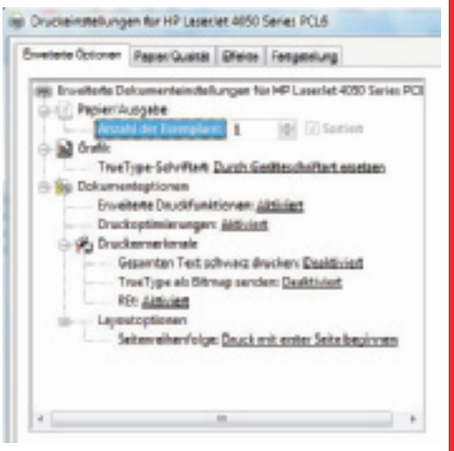


Druckeinstellungen

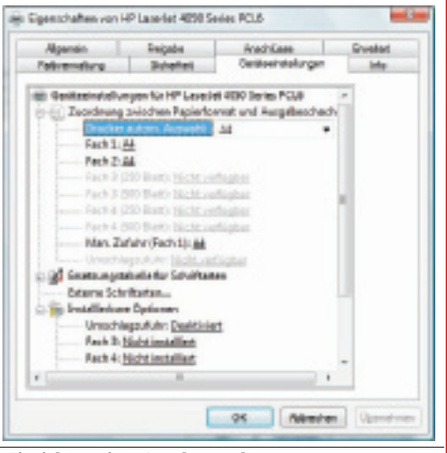
In den Eigenschaften jedes logischen Druckerobjekts können Druckeinstellungen konfiguriert werden. Typische Einstellungen betreffen das Papierformat oder die Reihenfolge, in welcher Seiten ausgedruckt werden sollen.



Unter *„Erweitert"* lassen sich noch weitere Parameter – abhängig vom verwendeten Druckermodell – konfigurieren.



Die Karteikarte *„Geräteeinstellungen"* enthält Konfigurationseinstellungen zu Papierschächten, Postscript-Optionen und Drucker-RAM.

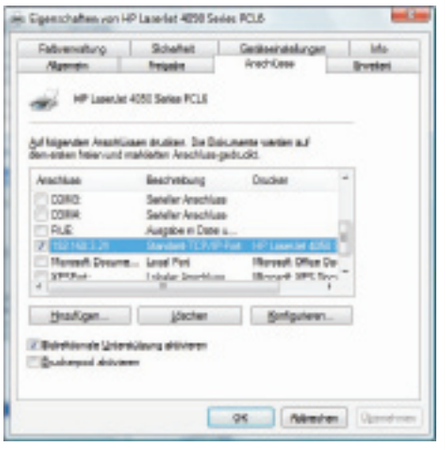


Einrichten eines Druckerpools

Unter einem Druckerpool versteht man mehrere gleichartige physische Drucker, die unter demselben Namen im Netzwerk angesprochen werden sollen. Es ist daher **ein** logisches Druckerobjekt zu erstellen, welchem **zwei** oder mehrere physische Drucker zugeordnet werden.

Dazu ist es nötig, zuerst einen der beiden Drucker wie beschrieben zu installieren und dann die Eigenschaften des logischen Druckerobjekts zu bearbeiten.

Zunächst muss ein zweiter Druckeranschluss hinzugefügt werden (da es sich in der Praxis meist um TCP/IP-Drucker handelt, sind in der Abbildung zwei TCP/IP-Ports dargestellt):

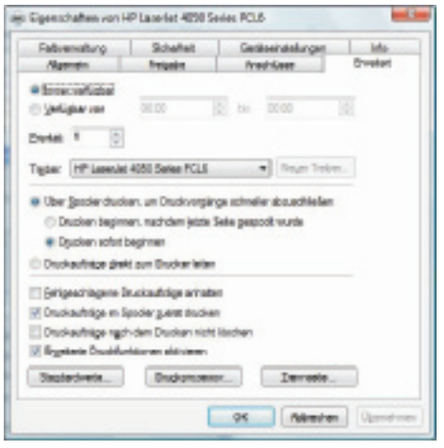


Danach muss die Einstellung *„Druckerpool aktivieren“* angekreuzt werden; beachten Sie, dass alle Anschlüsse, die zum Druckerpool gehören sollen, mit Kontrollkästchen aktiviert sein müssen!

Erweiterte Druckereigenschaften

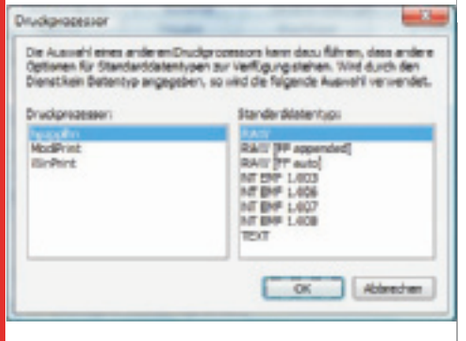
In der Karteikarte *„Erweitert“* kann konfiguriert werden:

- **Priorität der Druckaufträge** (zwischen 1 und 99): Aufträge mit geringerer Priorität werden in der Druckwarteschlage nachgereiht und daher später gedruckt.
- **Spooler umgehen**: Hier kann der Druckauftrag direkt zum Drucker gesendet werden. Das hat den Nachteil, dass der Druckvorgang länger dauert, da der im Drucker vorhandene RAM meist zu klein ist, um den kompletten Druckauftrag zwischenzuspeichern. Deshalb muss gewartet werden, bis der komplette Druckauftrag zum Drucker gesendet wurde, bevor weitergearbeitet werden kann.



- **Trennseite**: Hier ist es möglich, eine Trennseite für Druckaufträge zu konfigurieren, auf der Informationen wie der Benutzername des Auftraggebers enthalten sind.

- **Druckprozessor**: Hier kann die Verarbeitung von Grafiken geändert werden. Die voreingestellte Konfiguration *(WinPrint / RAW)* ist für viele Anwendungen ideal und muss nicht angepasst werden.



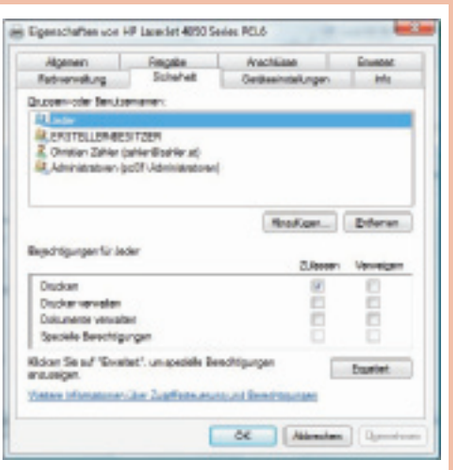
NTFS-Berechtigungen für logische Druckerobjekte

So wie für Dateien und Ordner können auch NTFS-Berechtigungen für logische Druckerobjekte erstellt werden.

Für Drucker existieren spezielle Berechtigungen:

- Drucken (das muss nicht speziell erklärt werden)
- Dokumente verwalten (mit dieser Berechtigung können Druckaufträge aus der Druckwarteschlange entfernt werden)
- Drucker verwalten (damit können logische Druckerobjekte umkonfiguriert werden)

Standardmäßig hat nur die Spezial-Identität `ERSTELLER-BESITZER` das Recht, Druckaufträge zu löschen. Das hat zur Folge, dass ein normaler Benutzer nur seine eigenen Druckaufträge aus der Warteschlange löschen kann, solange er nicht eine andere NTFS-Berechtigung bekommen hat.



Startvorgang, Datenträgerverwaltung und Notfallwiederherstellung

Startvorgang von Windows Vista

Die wichtigsten Komponenten während des Startvorgangs von Windows Vista findet man im Stammverzeichnis der Startpartition:

- **bootmgr**: Diese Applikation kontrolliert den Windows Vista Startvorgang. In einer Multiboot-Umgebung stellt bootmgr das Betriebssystem-Auswahlmenü dar. Bis Windows XP/Server 2003 war das Programm ntldr für diese Aufgaben verantwortlich.
- **Boot Configuration Data (BCD)**: Windows Vista speichert Startkonfigurationen in BCD. Das Programm `bootmgr` liest BCD, um das Betriebssystem-Auswahlmenü darstellen zu können. BDC ist der Nachfolger der Datei `boot.ini`, die in früheren Windows-Versionen verwendet wurde. Die Datenstruktur im BCD ist ähnlich wie ein Registry-Hauptschlüssel gespeichert und kann nicht direkt mit einem Texteditor bearbeitet werden.

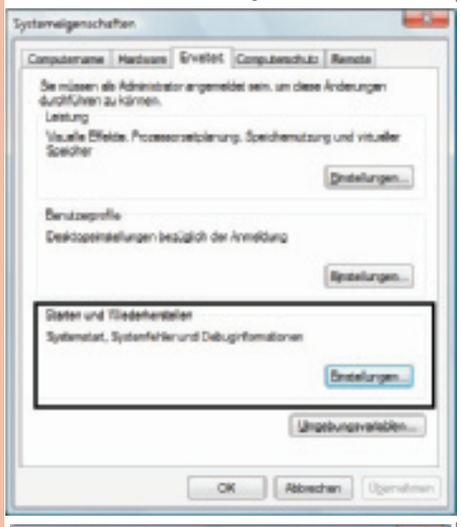
Beispiel (Quelle: `www.tecchannel.de`): Der BCD-Store enthält ein Objekt für den Bootmanager, zwei für Vista/Windows Server 2008 und einen für Windows XP/2000/2003.

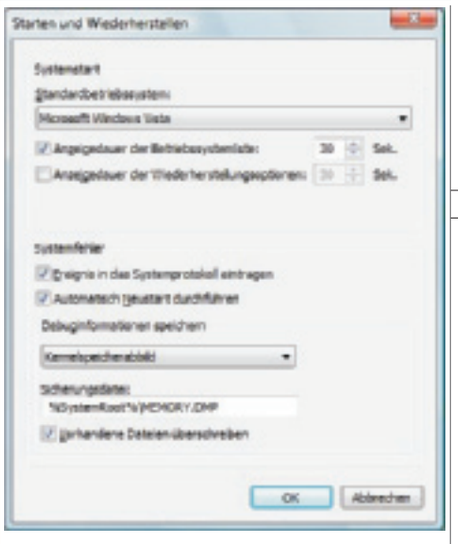
- `Winload.exe`: Dieses Programm lädt das Betriebssystem selbst. Fall aus dem Betriebssystem-Auswahlmenü Windows Vista ausgewählt wird, so wird die Kontrolle an `Winload.exe` übergeben. Es lädt den Kernel, das *Hardware Abstraction Layer* (HAL) und diverse Treiber in den Arbeitsspeicher. In einer Multiboot-Umgebung hat jede Windows Vista-Instanz ihren eigenen winload.exe.
- `Winresume.exe`: Das ist das *„Wiederaufnahme-Startprogramm“* für Windows Vista, falls das Betriebssystem aus dem Energiesparmodus wieder *(engl. „hibernation mode“)* in Betrieb genommen wird.

In früheren Windows-Versionen konnte die Datei `boot.ini` manuell mit jedem beliebigen Text-Editor verändert werden.

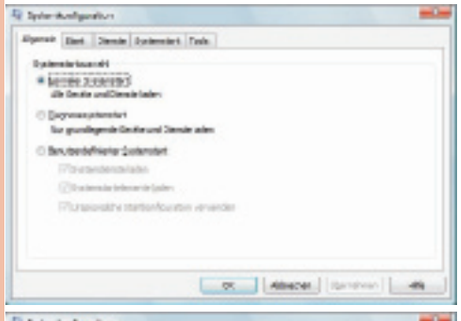
Der Startvorgang kann mit folgenden Methoden verändert werden:

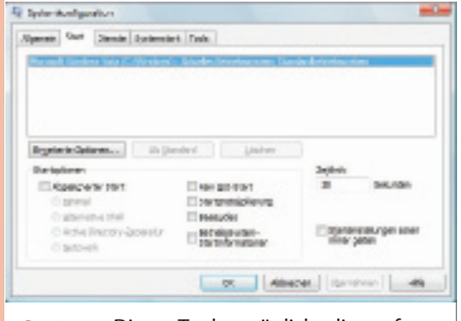
- *Systemeigenschaften*, Karteikarte *„Erweitert“*, Rubrik *„Start und Wiederherstellung“*:





- Systemkonfiguration (`msconfig.exe`)





- `BCDEdit`: Dieses Tool ermöglicht die umfangreichsten Konfigurationsmöglichkeiten („fast alle“) für den Startvorgang. Damit ist auch ein Export und Import von Konfigurationsdaten möglich.

Beispiel: Anzeige aktueller Konfigurationsdaten:

```
C:\>bcdedit /enum

Windows-Start-Manager
---------------------
Bezeichner              {bootmgr}
device                  partition=C:
description             Windows Boot Manager
locale                  de-DE
inherit                 {globalsettings}
default                 {current}
resumeobject
{a7cf2159-9ce5-11db-9b34-824fb58ca61f}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows-Startladeprogramm
-------------------------
Bezeichner              {current}
device                  partition=C:
path
\Windows\system32\winload.exe
description             Microsoft Windows Vista
locale                  de-DE
inherit                 {bootloadersettings}
osdevice                partition=C:
systemroot              \Windows
resumeobject
{a7cf2159-9ce5-11db-9b34-824fb58ca61f}
nx                      OptIn
```

- **Windows Management Interface (WMI)**: Diese Programmierschnittstelle ist die einzige Möglichkeit, kompletten Zugriff auf den BCD-Speicherbereich zu bekommen.

Backup und Restore, Notfallwiederherstellung

Backup

Windows Vista unterstützt Sie bei der Sicherung von PC-Einstellungen, Dateien und Anwendungen zum gewünschten Zeitpunkt und am gewünschten Speicherort und bietet eine automatische Zeitplanung. Windows Vista bietet eine umfassendere und auch benutzerfreundlichere Sicherungsumgebung als das einfache Sicherungsprogramm unter Windows XP. Das neue Feature *"Sicherung"* bietet mehr Optionen für das Speichern Ihrer gesicherten Informationen. Sie können Daten auf CD-ROM, DVD-ROM, einer externen Festplatte, die über USB oder IEEE 1394 am PC angeschlossen ist, einer anderen Festplatte im PC oder einem anderen mit dem Netzwerk verbundenen PC oder Server sichern.

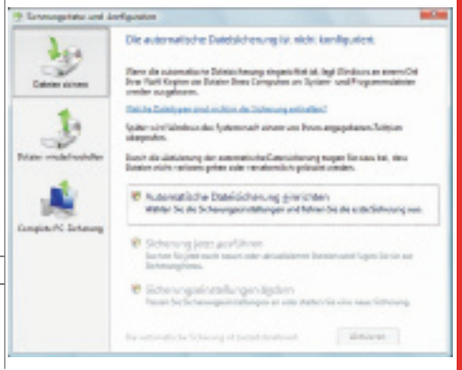
Unter Windows Vista ist der Sicherungsvorgang auch einfacher als unter Windows XP. Sie müssen Datensicherungen nicht mehr manuell durchführen, da es jetzt einen einfachen Assistenten gibt, mit dem Zeitpunkt und Speicherort von Sicherungen geplant werden können.

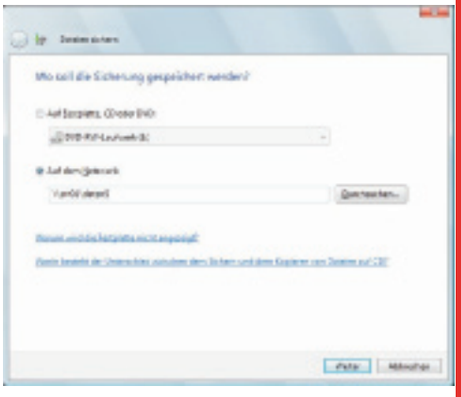
Eine Sicherungsumgebung ist freilich nur so nützlich wie die dazugehörige Wiederherstellungsumgebung, deren Umfang und Nutzen unter Windows Vista erweitert wurde. Ein Assistent hilft bei der Auswahl der wiederherzustellenden Dateien und Ordner und fordert die Angabe von Wiederherstellungsmedien an. Anschließend werden die ausgewählten Dateien wiederhergestellt.

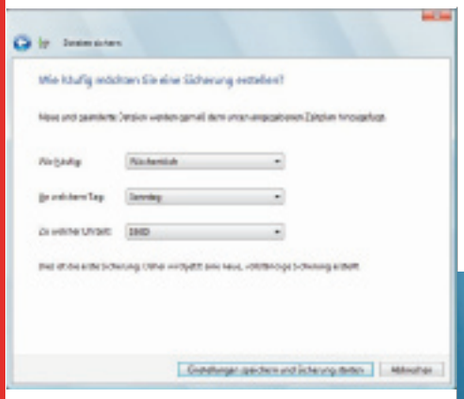
In der Systemsteuerung werden unter der Rubrik *„Sichern und Wiederherstellen“* grundsätzlich zwei Methoden vorgeschlagen:

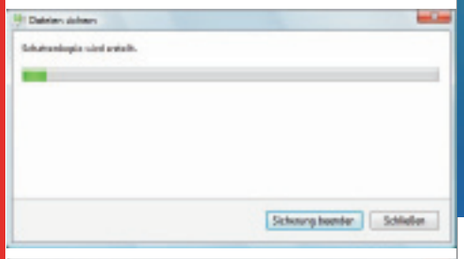
- Sicherung einzelner Dateien
- Sicherung des gesamten Computers

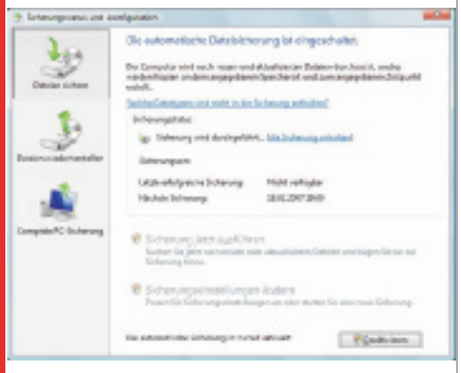
Die Sicherung einzelner Dateien erfolgt mit dem Assistenten *„Sicherungsstatus und -konfiguration“*:







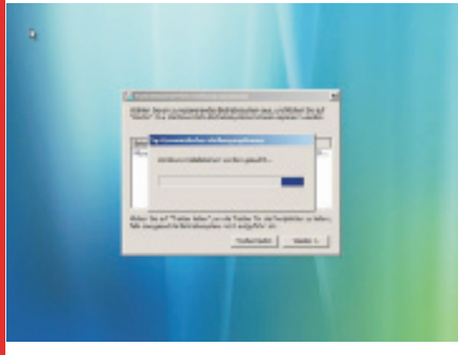




Aufbau des Backup-Verzeichnisses:

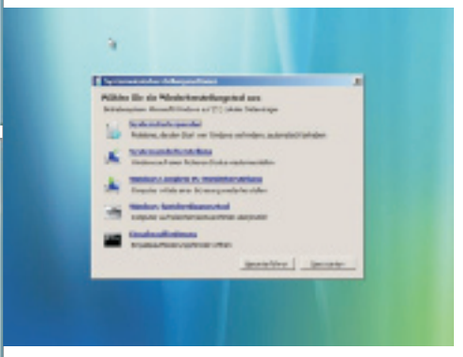
Startup Repair

Booten von DVD nötig, dann auf *„Reparieren"* klicken. Es werden dann die bestehenden Windows-Installationen gesucht:



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:

- **Systemreparatur**: Automatisches Reparieren von Windows Startproblemen (Bootsektor usw.)
- **Systemwiederherstellung**: Herstellen von Windows über vorhandene Wiederherstellungspunkte (Konfiguration von Wiederherstellungspunkten siehe nächstes Kapitel)
- **Windows komplette PC-Wiederherstellung**: Komplettes Wiederherstellen eines Windows-Backups
- **Windows-Speicherdiagnosetool**: Arbeitsspeicher auf Fehler überprüfen (Neustart erforderlich)
- **Eingabeaufforderung** (bis Windows XP/2003: *„Wiederherstellungskonsole"*): Kommandozeile/Eingabeaufforderung



In der Wiederherstellungskonsole stehen folgende Kommandos zur Verfügung:

Attrib ändert Attribute einer Datei oder eines Unterverzeichnisses.

Batch führt die in einer Textdatei angegebenen Befehle aus (Eingabedatei); Ausgabedatei enthält die Ausgabe der angegebenen Befehle. Wenn der Parameter Ausgabedatei nicht angegeben ist, wird die Ausgabe auf dem Bildschirm angezeigt.

Bootcfg dient zum Bearbeiten der Datei `Boot.ini` für die Startkonfiguration und die Wiederherstellung.

CD (Chdir) funktioniert nur innerhalb der Systemverzeichnisse der aktuellen Windows-Installation, auf Wechselmedien, im Stammverzeichnis einer Festplattenpartition oder in den lokalen Installationsverzeichnissen.

Chkdsk Der Parameter `/p` führt `Chkdsk` aus, auch wenn das Laufwerk als sauber markiert ist. Der Parameter `/r` sucht nach fehlerhaften Sektoren und stellt lesbare Daten wieder her; dieser Parameter impliziert `/p`. Chkdsk erfordert Autochk. Chkdsk sucht automatisch im Startverzeichnis nach `Autochk.exe`. Wenn Chkdsk die Datei nicht im Startverzeichnis finden kann, sucht Chkdsk nach der Windows-Installations-CD. Wenn Chkdsk die Installations-CD nicht finden kann, wird der Benutzer aufgefordert, den Pfad zur Datei `Autochk.exe` anzugeben.

Cls löscht den Bildschirminhalt.

Copy kopiert eine Datei in ein Zielverzeichnis. Das Ziel kann standardmäßig kein Wechselmedium sein, und es können keine Platzhalter verwendet werden. Beim Kopieren einer komprimierten Datei von der Windows-Installations-CD wird die Datei automatisch dekomprimiert.

Del (Delete) löscht eine Datei. Funktioniert nur innerhalb der Systemverzeichnisse der aktuellen Windows-Installation, auf Wechselmedien, im Stammverzeichnis einer Festplattenpartition oder in den lokalen Installationsverzeichnissen. Es können standardmäßig keine Platzhalter verwendet werden.

Dir zeigt eine Liste aller Dateien an, einschließlich versteckte und Systemdateien.

Disable deaktiviert einen Windows-Systemdienst oder -Treiber. Die Variable Dienst_oder_Treiber ist der Name des Dienstes oder Treibers, den Sie deaktivieren wollen. Wenn Sie diesen Befehl verwenden, um einen Dienst zu deaktivieren, wird der ursprüngliche Starttyp des Dienstes angezeigt, bevor der Typ in `SERVICE_DISABLED` geändert wird. Sie sollten sich den ursprünglichen Starttyp notieren, damit Sie den Befehl **Enable** verwenden können, um den Dienst wieder zu starten.

Diskpart verwaltet Partitionen auf Festplatten. Die Option `/add` erstellt eine neue Partition; die Option `/delete` löscht eine bestehende Partition. Die Variable Gerät ist der Gerätename für eine neue Partition (wie `\Gerät\Festplatte0`). Die Variable Laufwerk ist der Laufwerkbuchstabe für das Löschen einer bestehenden Partition (zum Beispiel `D`); Partition ist der Partitionsname für das Löschen einer bestehenden Partition (zum Beispiel `\Gerät\Festplatte0\Partition1`) und kann anstelle der Variable Laufwerk verwendet werden. Die Variable Größe ist die Größe einer neuen Partition in MB.

Enable aktiviert einen Windows-Systemdienst oder -Treiber. Die Variable `Dienst_oder_Treiber` ist der Name des Dienstes oder Treibers, den Sie aktivieren wollen, und `Starttyp` ist der Starttyp für einen aktivierten Dienst. Der Starttyp verwendet eines der folgenden Formate:

```
SERVICE_BOOT_START
SERVICE_SYSTEM_START
SERVICE_AUTO_START
SERVICE_DEMAND_START
```

Exit beendet die Wiederherstellungskonsole und startet den Computer neu.

Expand expandiert eine komprimierte Datei. Die Variable Quelle gibt die zu expandierende Datei an. Es können standardmäßig keine Platzhalter verwendet werden. Die Variable Ziel gibt das Verzeichnis für die neue Datei an. Das Verzeichnis kann standardmäßig kein Wechselmedium und kann nicht schreibgeschützt sein. Sie können den Befehl attrib verwenden, um den Schreibschutz des Zielverzeichnisses aufzuheben. Die Option `/f:filespec` ist erforderlich, wenn die Quelle mehr als eine Datei enthält; bei dieser Option können Platzhalter verwendet werden. Der Parameter `/y` deaktiviert die Bestätigungsaufforderung vor dem Überschreiben. Der Parameter `/d` gibt an, dass die Dateien nicht expandiert werden sollen und zeigt ein Verzeichnis der Dateien in der Quelle an.

Fixboot schreibt einen neuen Startsektor auf der Systempartition.

Fixmbr repariert den Master Boot Code der Startpartition. Die Variable Gerät ist ein optionaler Name, der das Gerät angibt, das einen neuen MBR benötigt; lassen Sie diese Variable weg, wenn das Ziel das Startgerät ist.

Format formatiert einen Datenträger. Der Parameter `/q` führt eine Schnellformatierung durch, der Parameter `/fs` gibt das Dateisystem an.

Help Wenn Sie nicht die Variable `Befehl` verwenden, um einen Befehl anzugeben, listet `help` alle Befehle auf, die die Wiederherstellungskonsole unterstützt.

Listsvc zeigt alle verfügbaren Dienste und Treiber auf dem Computer an.

Logon zeigt erkannte Windows-Installationen an und fordert die Eingabe des lokalen Administratorkennworts für diese Installationen. Verwenden Sie diesen Befehl, um zu einer an-

deren Installation oder einem anderen Unterverzeichnis zu wechseln.

Map zeigt die aktiven Gerätezuordnungen an. Fügen Sie die Option arc ein, um Advanced RISC Computing (ARC)-Pfade (das Format für `Boot.ini`) statt Windows-Gerätepfade zu verwenden.

MD (Mkdir) funktioniert nur innerhalb der Systemverzeichnisse der aktuellen Windows-Installation, auf Wechselmedien, im Stammverzeichnis einer Festplattenpartition oder in den lokalen Installationsverzeichnissen.

More/Type zeigt die angegebene Textdatei (z.B. den Dateinamen) auf dem Bildschirm an.

Rd (Rmdir) funktioniert nur innerhalb der Systemverzeichnisse der aktuellen Windows-Installation, auf Wechselmedien, im Stammverzeichnis einer Festplattenpartition oder in den lokalen Installationsverzeichnissen.

Ren (Rename) funktioniert nur innerhalb der Systemverzeichnisse der aktuellen Windows-Installation, auf Wechselmedien, im Stammverzeichnis einer Festplattenpartition oder in den lokalen Installationsverzeichnissen. Sie können kein neues Laufwerk/keinen neuen Pfad als Ziel angeben.

Set dient zur Anzeige und Definition der Umgebungsvariablen der Wiederherstellungskonsole.

Systemroot setzt das aktuelle Verzeichnis auf `%SystemRoot%`.

MRT Microsoft Tool zum Entfernen bösartiger Software. Dieses Tool überprüft, ob Trojaner auf Ihrem Rechner vorhanden sind.

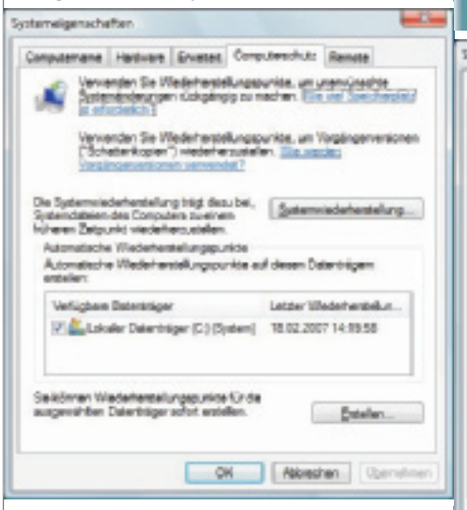
Systemwiederherstellung und Volumenschattenkopien („Volume Shadow Copies")

Die Systemwiederherstellung wurde unter Windows XP eingeführt, damit Benutzer ihre Computer in einen vorherigen Zustand zurückversetzen können, ohne persönliche Datendateien zu verlieren (wie z. B. Microsoft Office Word-Dokumente, Grafikdateien und E-Mail-Nachrichten). Für die Systemwiederherstellung müssen keine Systemsnapshots erstellt werden, da das System einfach erkennbare 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 Vista 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 Vista 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 Vista verwendete Volume kopiert. Dadurch wird die Integration mit anderen Aspekten der Sicherung und Wiederherstellung verbessert und die Systemwiederherstellungsfunktion noch nützlicher.

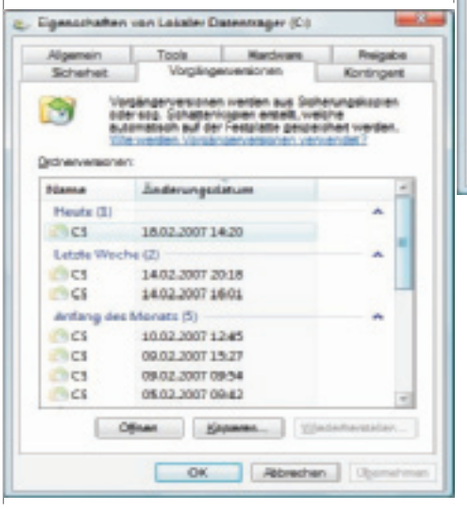
Aktivieren des Computerschutzes: Unter *Systemeigenschaften – Computerschutz*:



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.

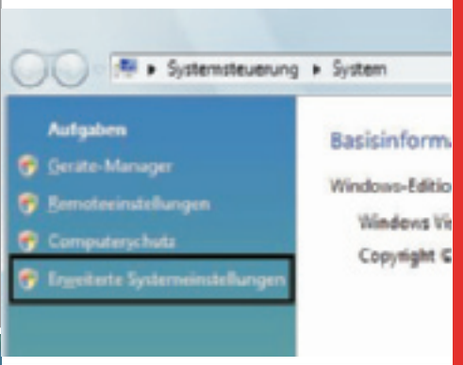
Klicken Sie mit der rechten Maustaste auf die Datei bzw. den Ordner, und klicken Sie dann auf Vorherige Versionen wiederherstellen.

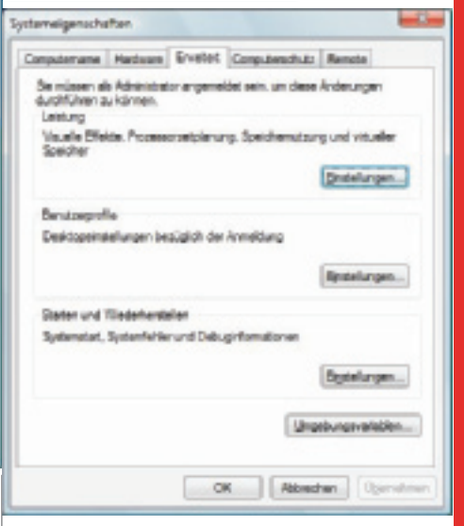
Es wird eine Liste der verfügbaren vorherigen Datei- oder Ordnerversionen angezeigt. Die Liste enthält sowohl Sicherungs- als auch Schattenkopien, sofern beide Typen vorhanden sind.



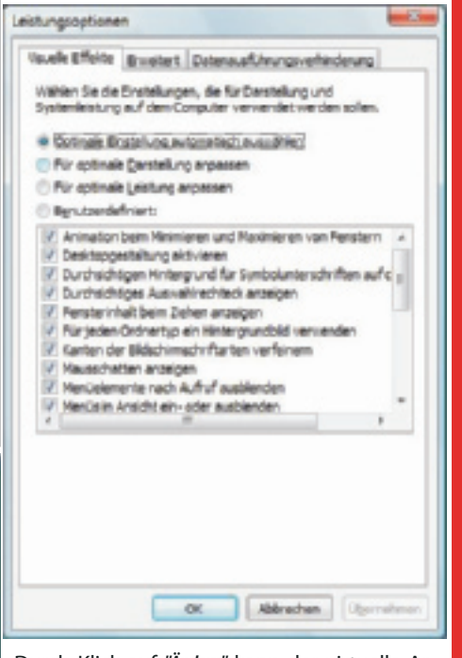
Die Systemeigenschaften von Windows Vista

Aufrufen mit *„Windows-Taste/PAUSE"* oder in der Systemsteuerung.



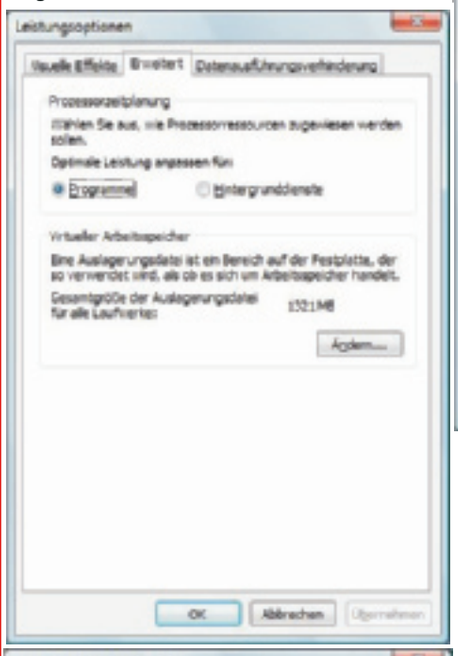


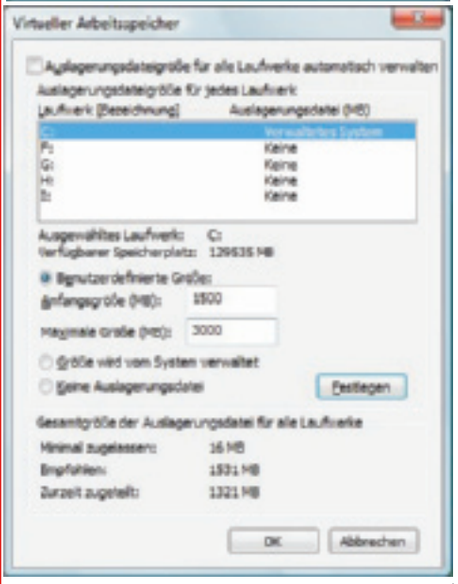
Systemleistungsoptionen



Durch Klick auf *"Ändern"* kann der virtuelle Arbeitsspeicher (d.h. Größe der Auslagerungsdatei, engl. *Swap File*) geändert werden.

Empfohlene Größe der Auslagerungsdatei: etwa 1,5x des installierten Hauptspeichers (mehr hat keinen Sinn, da sonst Performance-Verluste auftreten!). Braucht man mehr, so ist es sinnvoller, physischen Speicherplatz zu ergänzen.





Windows NT-Betriebssysteme unterstützen einen 32-Bit-Adressraum, das bedeutet einen virtuellen Adressbereich von 4 GB. Jedem Programm wird ein solcher virtueller 4 GB-Adressraum zugeordnet. (Hätte man diesen Speicher auch physikalisch, so könnte das Programm diesen Speicher auch nutzen!)

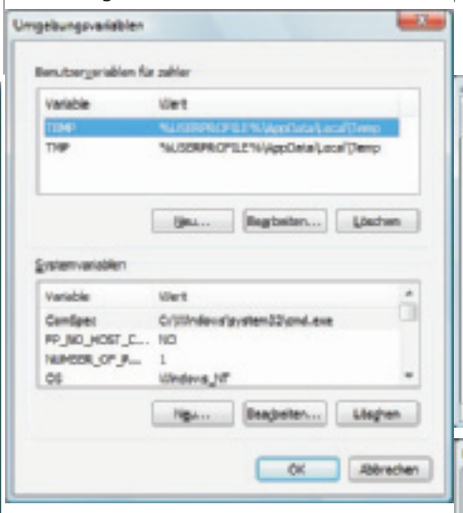
Die Zuordnung zwischen tatsächlich vorhandenem Speicher und virtuellem Speicher wird vom VMM = *Virtual Memory Manager* durchgeführt.

Ist für mehrere Programme eine Zuweisung von tatsächlichem RAM nicht mehr möglich (*Page Fault* = Seitenzuordnungsfehler), so muss ein Teilbereich aus dem RAM auf die Festplatte ausgelagert werden. Damit werden diese Daten auf die "Swap-Datei" (Auslagerungsdatei) auf die Festplatte ausgelagert.

Die Auslagerung erfolgt generell in 4 KB-Blöcken.

Umgebungsvariablen

Altes Konzept, mit dem Programme (älteren Datums) gesteuert werden können.



Die Umgebungsvariablen können in der Kommandozeile abgefragt werden:

```
echo %ComSpec%
```

Diese Variablen können auch gesetzt werden:

```
set werbinich=Zahler
echo %werbinich%
```

Mit `set` können alle Umgebungsvariablen ausgelesen werden:

```
C:\Users\zahler>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\zahler\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common
Files
COMPUTERNAME=PC01
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=Z:
HOMEPATH=\
HOMESHARE=\\dc01\user\zahler\home
LOCALAPPDATA=C:\Users\zahler\AppData\Local
LOGONSERVER=\\DC01
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\
System32\Wbem;C:\Program Files\Wi
ndows Imaging\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;
.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 15 Model 4
Stepping 9, GenuineIntel
PROCESSOR_LEVEL=15
PROCESSOR_REVISION=0409
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
PROMPT=$P$G
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\zahler\AppData\Local\Temp
TMP=C:\Users\zahler\AppData\Local\Temp
USERDNSDOMAIN=ZAHLER.AT
USERDOMAIN=ZAHLER
USERNAME=zahler
USERPROFILE=C:\Users\zahler
windir=C:\Windows
```

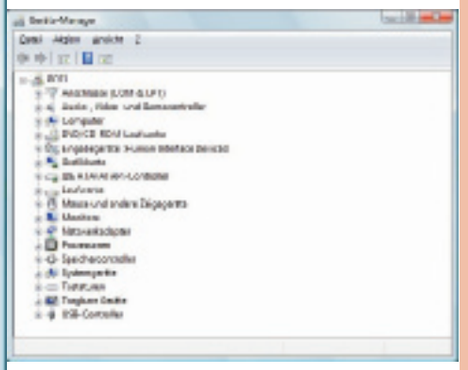
Starten und Wiederherstellen

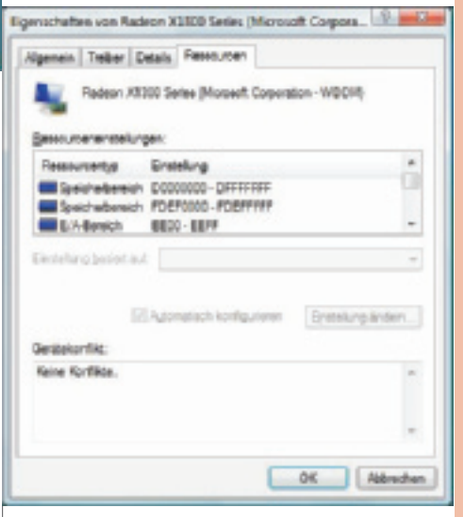
Siehe Kapitel *„Startvorgang"*!

Treiber und Hardware-Installation

Geräte-Manager

Wird meist im Gerätemanager durchgeführt, dieser ist über das Kontextmenü des Arbeitsplatzes erreichbar.



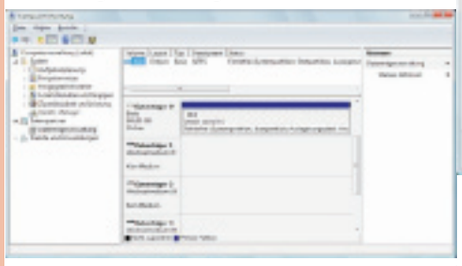


Ressourcenverwaltung:

- IRQ
- E/A-Speicherbereich
- RAM-Speicherbereich
- bei manchen Geräten: DMA-Kanal (zum Beispiel Diskettenlaufwerkscontroller)

Tools zur Verwaltung von Festplatten

Datenträgerverwaltung



Die Betriebssysteme Windows 2000/XP/2003/Vista unterstützen zwei Arten der Festplattenverwaltung:

- **Basisdatenträger:** Hier wird ein zu anderen Systemen kompatibler Master Boot Record erstellt und verwaltet. Daher gibt es für Basisdatenträger die Beschränkung auf max. 4 Partitionseinträge in den MBR. Auf Basisdatenträgern können bootfähige primäre und nicht bootfähige erweiterte Paritionen angelegt werden. Um erweiterte Partitionen für die Datenspeicherung nützen zu können, müssen innerhalb dieser Partitionen noch „logische Laufwerke" definiert werden.
- **Dynamische Datenträger**: Proprietäres Microsoft-System, nicht kompatibel mit anderen Betriebssystemen (auch nicht mit Windows 9x oder NT 4.0). Nur auf dynamischen Datenträgern können RAID- oder übergreifende Laufwerke angelegt werden.

Basisdatenträger können ohne Datenverlust in dynamische Datenträger konvertiert werden; der umgekehrte Vorgang ist aber nicht möglich (es würde eine Neupartitionierung erfolgen, die alle bestehenden Daten unzugänglich macht).

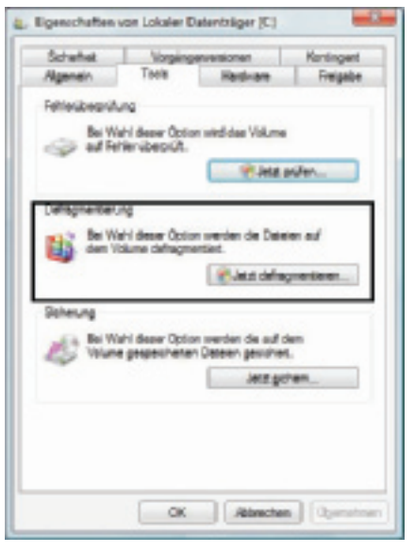
Defragmentierung

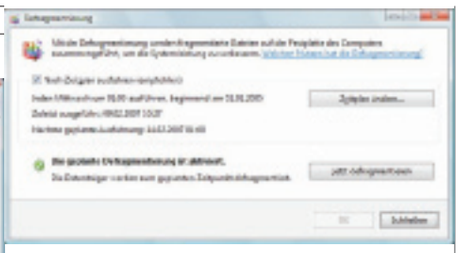
- **Befehlszeilentool defrag** (Windows XP/2003)

Syntax:

```
defrag <Volume> [-a] [-f] [-v] [-?]
  Volumelaufwerkbuchstabe oder
Bereitstellungspunkt (d: oder
d:\vol\mountpoint)
  -a      Nur analysieren
  -f      Erzwingt das Defragmentieren auch bei
niedrigem Speicher.
  -v      Ausführliche Ausgabe
  -?      Zeigt die Hilfe an.
```

- **Grafisches Tool**





Partitionierung

- **Befehlszeilentool** `diskpart` (Windows XP/2003)
- **MMC-Snap-In** *„Datenträgerverwaltung"*
- **Drittanbieter-Tools:** Damit sind auch Nicht-Windows-Partitionen (etwa für Multiboot-Umgebungen) einrichtbar.

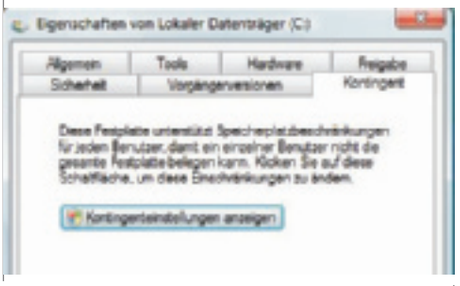
Bekannt ist etwa Symantec PartitionMagic (mit integriertem Bootmanager BootMagic).

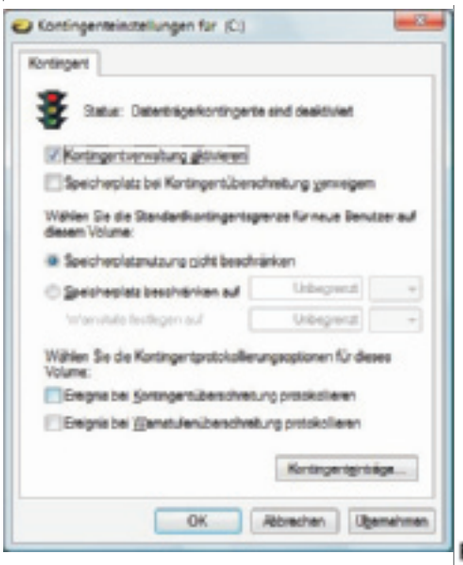
Formatierung

- **Befehlszeilentool** `format`
- **MMC-Snap-In** *„Datenträgerverwaltung"*

Einrichtung von Datenträgerkontingenten (Disk Quota)

- **MMC-Snap-In** *„Datenträgerverwaltung"*





- **Befehlszeilentool** `fsutil` (Windows XP/2003)

Beispiel für die Abfrage von Informationen mit `fsutil`:

```
fsutil fsinfo ntfsinfo C:
NTFS-Volumeseriennummer :
0x94708419708403e8
Version :                          3.1
Anzahl der Sektoren :
0x000000000445c7ae
Gesamtzahl Cluster :
0x000000000088b8f5
Freie Cluster :
0x00000000007a1800
Insgesamt reserviert :
0x0000000000007f10
Bytes pro Sektor :                 512
Bytes pro Cluster :                4096
Bytes pro Dateidatensatzsegment :  1024
Cluster pro Dateidatensatzsegment : 0
MFT-gültige Datenlänge :
0x0000000000d0fc00
MFT-Start-LCN :
0x0000000000c0000
MFT2-Start-LCN :
0x0000000000445c7a
MFT-Zonenstart :
0x0000000000c0ae0
MFT-Zoneende :
0x0000000001d1720
```

RAID *(Redundant Array of Inexpensive Disks)*

Konzept

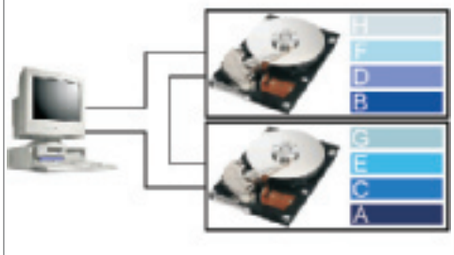
Wächst das Netz, so steigen auch die Anforderungen an Sicherheit und Geschwindigkeit der Massenspeicher. Die heutigen Festplatten haben eine MTBF (*mean time between failures*, mittlerer Störabstand) von über 15 Jahren. Die typischen Zugriffszeiten liegen unter 10 ms. Dies bedeutet aber nicht, dass an sich bedingungslos auf diese Massenspeicher verlassen kann. Um nun den Datenzugriff zu beschleunigen und die Datensicherheit zu erhöhen, haben 1987 die Professoren Gibson, Katz und Patterson der Berkeley University den RAID-Standard *(Redundant Arrays of Inexpensive Disks)* definiert. Dieser Standard enthält verschiedene Definitionen, welche die Geschwindigkeit und die Zuverlässigkeit von Massenspeichern erhöhen. Dies geschieht in der Praxis durch überlappende Schreib- und Lesezugriffe.

RAID Level 0: Block Striping

Block Striping bedeutet, dass einzelne Datenblocks über mehrere Disks verteilt werden, also quasi in "Streifen" zerlegt werden. So kann z.B. eine 20 GB Festplatte in vier Teile zu je 5 GB aufgeteilt werden, so dass die Daten wie folgt verteilt sind:

Die Blockgröße (Striping Depth) beträgt in den meisten Fällen 8kB, kann jedoch von 2 bis 32 kB gehen. Dateien, die größer als 8 kB sind, werden automatisch auf mehrere Disks aufgeteilt. Je nach gewählter Implementation werden mehrere kleine Files in einen Block (Speicheroptimierung) oder jedes File immer in einem eigenen block (Geschwindigkeitsoptimierung) abgelegt. Fällt allerdings ein Laufwerk aus, so sind in aller Regel die dort gespeicherten Segmente verloren und somit die Daten des gesamten Arrays unbrauchbar. Deshalb trägt RAID Level 0 den Namen *Redundant Array* eigentlich zu Unrecht, da die Daten nicht mehrfach gespeichert werden und das Array somit keine Fehlertoleranz bietet. RAID 0 ist für Anwendungen interessant, bei denen ein hoher Datendurchsatz benötigt wird, ohne dass dabei die kontinuierliche Sicherheit von besonderer Bedeutung ist.

RAID 0 (Striping)



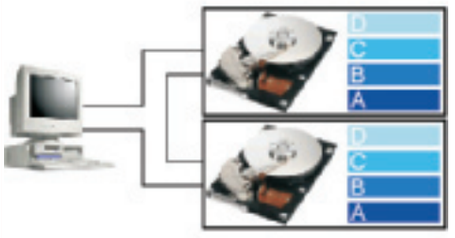
© tecChannel.de

RAID Level 1: Disk Mirroring bzw. Disk Duplexing

Disk Mirroring bedeutet, dass zwei oder mehrere Disks genau dieselben Daten enthalten. Dabei wird aber der gleiche Controller verwendet. Wenn sowohl Controller als auch Disks doppelt vorhanden sind, so wird das so genannte *Disk Duplexing* realisiert:

Jede Information ist also doppelt auf den Festplatten gespeichert, wodurch sich die Schreibvorgänge etwas verlängern. Die Verteilung (bzw. die Verdoppelung) der Daten wird dabei wie folgt vorgenommen:

RAID 1 (Mirroring)



© tecChannel.de

Das Lesen von Daten kann auf verschiedene Arten vonstatten gehen:

- Alle Daten werden von der ersten Disk gelesen, währen die zweite Disk nur als Backup-Disk dient.
- Die Daten werden alternierend von einer oder von der anderen Disk gelesen.
- Eine Leseanfrage wird an alle Disks geleitet; die erste antwortende Disk wird berücksichtigt. (Diese Vorgehensweise wurde von Novell bis zur NetWare Version 3.1 implementiert.)
- Die Daten werden normalerweise von der ersten Disk gelesen. Ist diese beschäftigt, so kommt die zweite Disk zum Zuge. (Diese Vorgehensweise ist von Novell in den Versionen 3.11 und 3.12 sowie 4.x implementiert.)

Beim Schreiben der Daten unter RAID 1 gibt es ebenfalls verschiedene Möglichkeiten:

- Die erste Disk wird sofort beschrieben, während die zweite Disk erst dann einen Schreibauftrag erhält, wenn sie nicht mehr beschäftigt ist.
- die Daten werden sofort auf beide Disks geschrieben; sobald beide Disks fertig sind, geht die Verarbeitung weiter. Diese zwar etwas langsamere Art bietet eine hohe Datensicherheit (wird von NetWare angewendet).

Obwohl RAID 1 die Verdoppelung der Speicherkapazität und damit der Kosten bedeutet, handelt es sich dabei um die am häufigsten implementierte Variante. In der Tat funktioniert RAID 1 bereits mit zwei Festplatten.

Dabei setzt RAID auf eines der ältesten Verfahren zur Fehlerkorrektur, die Paritätsprüfung. Dazu verknüpft es die Daten der Nutzlaufwerke über eine logische Exklusiv-Oder-Operation (XOR) und speichert das Resultat auf einem eigenen Parity-Laufwerk. Das Ergebnis der Verknüpfung ist dann 1, wenn eine ungerade Anzahl von Bitstellen eine 1 aufweist. Bei einer geraden Anzahl dagegen ist das Ergebnis 0:

Parity-Generierung

Laufwerk	Inhalt
Laufwerk A	11101100
Laufwerk B	10110011
Laufwerk C	01001101
Parity-Laufwerk	00010010

Fällt nun ein beliebiges Laufwerk aus, lassen sich durch ein erneutes XOR die verloren gegangenen Daten problemlos rekonstruieren:

Fehlerkorrektur durch Parity

	vor dem Ausfall	Ausfall Datenlaufwerk	Ausfall Parity-Laufwerk
Laufwerk A	11101100	11101100	11101100
Laufwerk B	10110011	xxxxxxx	10110011
Laufwerk C	01001101	01001101	01001101
Parity-Laufwerk	00010010	00010010	xxxxxxx
Datenrekonstruktion		10110011	00010010

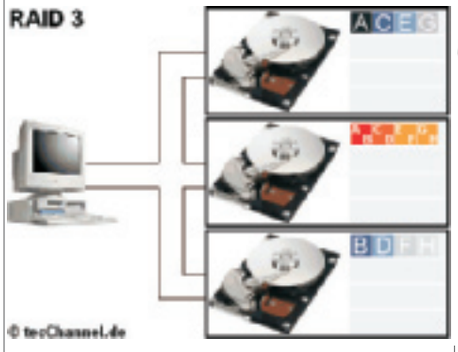
RAID Level 2: Interleaving

Bei dieser Variante von RAID werden die Daten nach dem Interleaving-Verfahren gespeichert. Das erste Segment einer Datei wird auf der ersten Festplatte abgelegt, das zweite Segment auf der zweiten und so weiter. Parallel dazu enthaltene mehrere zusätzliche Platten Prüfnummern und Zusatzinformationen, die im Notfall zur Rekonstruktion der Daten notwendig sind. RAID Level 2 hat im Netzwerkbereich praktisch keine Bedeutung und wird nur auf Großrechnern verwendet; aus diesem Grund wird auf eine weitergehende Darstellung verzichtet.

RAID Level 3: Synchronised Spindles

Bei RAID 3 arbeiten alle Festplatten parallel (synchronisiert). Eine separate Festplatte wird für die Paritätsinformationen verwendet, die im Notfall die Rekonstruktion der Daten erlaubt. So kann bei Ausfall einer Platte die Information mit Hilfe der restlichen Platten rekonstruiert werden.

RAID 3



© tecChannel.de

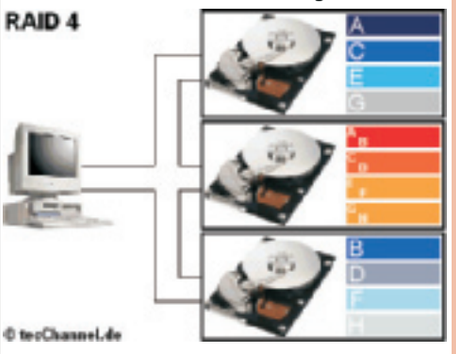
Die Datenübertragungsgeschwindigkeit ist bei RAID 3 bis zu 4 Mal höher als bei einer einzelnen Disk, allerdings auf Kosten der Lesegeschwindigkeit, da die Steuerung immer nur einen Lesebefehl abarbeiten kann. Da die Dateien in kleinen Teilen über alle Platten verteilt sind, ist RAID 3 interessant für Anwendungen mit wenigen, aber sehr großen Dateien (z.B. Graphik, große Datenbanken, etc.). Für häufigen Zugriff auf kleine Dateien oder für intensiven Multitaskingbetrieb sollte RAID 3 nicht angewendet werden, da ein Lesevorgang alle Festplatten blockiert.

RAID Level 4: Block Striping with Parity

Raid Level 4 entspricht RAID 0 mit zusätzlicher Parity. Dies bedeutet, dass die einzelnen Datenblocks über mehrere Disks verteilt werden und eine zusätzliche Disk für die Paritätsinformationen eingesetzt wird.

Die Lesegeschwindigkeit ist dieselbe wie bei RAID 0 und theoretisch vier Mal schneller der einen einzelnen Festplatte. Die Schreiboperationen erfolgen jedoch relativ langsam, da das System nur einen Schreibvorgang nach dem anderen abarbeiten kann und zum Errechnen der Paritätsinformationen zuerst die Daten gelesen werden müssen. RAID 4 eignet sich da-

RAID 4



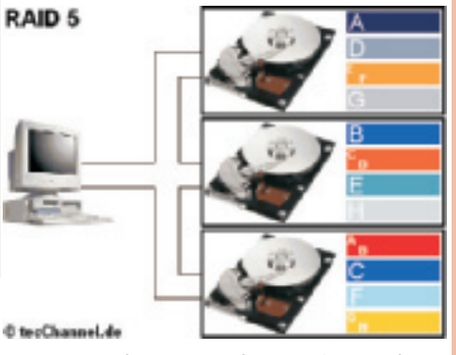
© tecChannel.de

her für Anwendungen, bei denen viel gelesen, aber wenig geschrieben wird.

RAID Level 5: Block Striping with Distributed Parity

RAID 5 begegnet dem Problem der langsamen Schreibvorgänge unter RAID 4 mit dem Schreiben der Paritätsinformationen auf allen Disks (selbstverständlich werden die Daten nicht auf der gleichen Festplatte abgelegt wie die Paritätsinformationen):

RAID 5



© tecChannel.de

RAID 5 wird unter Windows NT/2000 relativ häufig eingesetzt, da es prozentual weniger Speicher „vergeudet" und zudem für Lesevorgänge eine erhöhte Performance bietet.

RAID Level 6/7: Block Striping and Block Mirroring (Exoten, sind unbedeutend)

RAID 6 stellt einen Versuch dar, gegenüber RAID 3 bis 5 die Ausfallsicherheit nochmals zu erhöhen. Bei diesen Verfahren darf nur eine Platte des Arrays ausfallen, da sich sonst die Daten nicht mehr per XOR rekonstruieren lassen. RAID 6 umgeht diese Einschränkung, indem es quasi ein RAID 5 um eine zusätzliches Parity-Laufwerk ergänzt. Zwar dürfen nun zwei Platten des Verbunds ausfallen, ohne dass Datenverluste auftreten. Die zusätzliche Sicherheit muss allerdings mit gegenüber RAID 3 bis 5 deutlich langsameren Schreibzugriffen erkauft werden.

Auch das proprietäre RAID 7 ist ähnlich wie RAID 5 aufgebaut. Allerdings setzt der Hersteller Storage Computer im Controller zusätzlich ein lokales Echtzeitbetriebssystem ein. Schnelle Datenbusse und mehrere große Pufferspeicher koppeln die Laufwerke vom Bus ab. Dieses asynchrone Verfahren soll Lese- wie Schreiboperationen gegenüber anderen RAID-Varianten erheblich beschleunigen. Zudem lässt sich, ähnlich wie bei RAID 6, die Paritätsinformation auch auf mehrere Laufwerke speichern.

Einsatz

Für den Einsatz der RAID-Technologie spricht, dass mehrere kleine Festplatten schneller sind als eine große Festplatte. Allerdings ist ein sol-

ches System störungsanfälliger, weshalb spezielle Sicherheitsmaßnahmen getroffen werden müssen. In keinem Fall darf aber ein RAID-System als Ersatz für einen regelmäßigen Backup angesehen werden. Grundsätzlich gilt, dass Data Striping die Leistungsfähigkeit stark verbessern kann, während! Data Duplexing den besten Datenschutz bietet. Neben den oben angesprochenen Hardwarelösungen gibt es für gewisse Fälle auch Softwarelösungen, die aber hier nicht weiter besprochen werden sollen.

Welcher RAID-Level gewählt werden soll, hängt von der Menge und Art der zu speichernden Daten ab. Folgende Fragen sollten gestellt werden:

- Wie wichtig – d.h. sicherheitsrelevant – sind Daten?
- Wie oft muss auf die Daten zugegriffen werden?
- Handelt es sich um wenige große oder viele kleine Dateien?

© tecChannel.de

Die folgende Tabelle enthält einen Überblick über die verschiedenen Levels; als Vergleichsgröße beim Schreiben, Lesen und notwendigen Speicherplatz dient eine einfache Festplatte, während bei den Anwendungen die Eignung angegeben wird („+" oder „++" heißt schneller bzw. geeignet, „-„ oder „- -„ heißt langsamer bzw. ungeeignet).

Level	Schreibvorgänge	Lesevorgänge	gebotene Sicherheit	Zusätzlicher Speicherplatz	Komplexe Anwendungen
Festplatte	0	0	--		++
RAID 0	++	++	--	gleich	++
RAID 1	+	+	++	doppelte Kapazität	+
RAID 2	--	++	++	mind. 2 Zusatzplatten	--
RAID 3	+	--	++	eine Zusatzplatte	--
RAID 4	-	++	++	eine Zusatzplatte	++
RAID 5	+	++	++	eine Zusatzplatte	++
RAID 6	++	++	++	doppelte Kapazität	+

Unabhängig vom gewählten Level sollten moderne RAID-Systeme über zusätzlichen Sicherheits- und Überwachungsmechanismen verfügen. Solche Mechanismen umfassen beispielsweise die Möglichkeit des *„Hot Mounting"* (Austausch im laufenden Betrieb) und der laufenden Überprüfung des Zustandes der Festplatten. Ein weiteres Merkmal von modernen RAID-Systemen ist die Integration von eigenem Cache-Speicher, der die Leistungsfähigkeit stark erhöhen kann.

RAID-Implementierungen in Windows 2000/XP/2003

Um den Zugriff auf Daten bei Ausfall einer Festplatte zu erhalten, bietet Windows 2000 Server eine Softwareimplementierung einer Fehlertoleranztechnologie, die RAID *(Redundant Array of Independent Disks)* genannt wird. RAID stellt eine Fehlertoleranz durch die Implementierung einer Datenredundanz bereit. Die Datenredundanz sorgt dafür, dass ein Computer Daten auf mehr als einen Datenträger schreibt, wodurch die Daten bei Ausfall einer der Festplatten geschützt sind.

Sie können die RAID-Fehlertoleranz als Software- oder Hardwarelösung implementieren.

Software-RAID-Implementierungen

Windows 2000 Server unterstützt zwei Softwareimplementierungen von RAID: gespiegelte Datenträger (RAID 1) und Stripesetdatenträger mit Parität (RAID 5). Sie können neue RAID-Datenträger jedoch nur auf dynamischen Festplatten von Windows 2000 erstellen.

Bei Softwareimplementierungen von RAID ist eine Fehlertoleranz nach einem Ausfall erst möglich, wenn der Fehler behoben wurde. Tritt ein zweiter Fehler auf, ehe die Daten des ersten Fehlers wiederhergestellt wurden, können Sie die Daten nur aus einer Sicherung wiederherstellen.

Anmerkung: Bei einer Aktualisierung von Windows NT 4.0 auf Windows 2000 werden vorhandenen gespiegelte Datenträger und Stripesets mit Parität beibehalten. Windows 2000 bietet eine eingeschränkte Unterstützung dieser Fehlertoleranzsätze, d.h. sie können diese verwalten und löschen.

Alle RAID-Implementierungen von Windows 2000/2003 setzen dynamische Datenträger voraus!

Hardware-RAID-Implementierungen

Bei einer Hardwarelösung ist der Datenträgercontroller für das Erstellen und Wiederherstellen redundanter Informationen verantwortlich. Einige Hardwarehersteller implementieren einen RAID-Datenschutz direkt in ihre Hardware, z.B. mit Hilfe von Controllerkarten für Datenträgersätze. Da diese Methoden herstellerspezifisch sind und die Treiber der Fehlertoleranzsoftware des Betriebssystems umgehen, sind sie leistungsfähiger als Softwareimplementierungen von RAID. Darüber hinaus bieten Hardware-RAID-Implementierungen weitere Funktionen, wie z.B. zusätzliche fehlertolerante RAID-Konfigurationen, den Austausch fehlerhafter Festplatten im laufenden Betrieb, Reservelaufwerke für die Online-Umschaltung im Fehlerfall und dedizierten Zwischenspeicher zur Verbesserung der Leistung.

Anmerkung: Der in einer Hardwareimplementierung unterstützte RAID-Grad ist abhängig vom Hardwarehersteller.

Berücksichtigen Sie bei einer Entscheidung für eine Software- oder Hardware Implementierung von RAID die folgenden Punkte:

- Hardwarefehlertoleranz ist teurer als Softwarefehlertoleranz.
- Hardwarefehlertoleranz bietet in der Regel eine schnellere Datenträger-E/A als Softwarefehlertoleranz.
- Hardwarefehlertoleranzlösungen können die Geräteoptionen auf einen einzelnen Hersteller beschränken.
- Hardwarefehlertoleranzlösungen ermöglichen u.U. den Austausch von Festplatten bei laufendem Betrieb, ohne dass der Computer heruntergefahren werden muss, und Reservelaufwerke, die bei einem Fehlerfall automatisch aktiviert werden.

Gespiegelte Datenträger

Ein gespiegelter Datenträger nutzt den Fehlertoleranztreiber von Windows 2000/2003 Server (`ftdisk.sys`), um dieselben Daten gleichzeitig auf je ein Laufwerk auf zwei physischen Festplatten zu schreiben. Die beiden Laufwerke werden als Mitglieder des gespiegelten Datenträgers betrachtet. Das Implementieren eines gespiegelten Datenträgers sorgt für den Erhalt von Daten, wenn ein Mitglied des gespiegelten Datenträgers fehlerhaft sein sollte.

Ein gespiegelter Datenträger kann beliebige Partitionen enthalten, einschließlich der Start- oder Systempartition. Die Laufwerke eines gespiegelten Datenträgers müssen jedoch dynamische Windows 2000/2003-Laufwerke sein.

Gespiegelte Datenträger können als Stripesets auf mehrere Laufwerke verteilt werden. Diese Konfiguration wird häufig RAID 10 genannt, RAID 1 (Spiegelung) und RAID 0 (Striping). Im Gegensatz zu RAID 0 ist RAID 10 eine fehlertolerante RAID-Konfiguration, da jeder Datenträger im Stripeset auch gespiegelt wird. RAID 10 verbessert die Datenträger-E/A, indem Lese- und Schreibvorgänge im gesamten Stripeset ausgeführt werden.

Leistung gespiegelter Datenträger

Gespiegelte Datenträger können die Leseleistung verbessern, da der Fehlertoleranztreiber Daten beider Mitglieder des Datenträgers gleichzeitig liest. Die Schreibleistung ist geringfügig schwächer, da der Fehlertoleranztreiber Daten auf beide Mitglieder schreiben muss. Fällt eines der Laufwerke eines gespiegelten Datenträgers aus, bleibt die Leistung normal, da der Fehlertoleranztreiber nur in einer Partition arbeitet.

Da die Speichernutzung nur 50 % beträgt (da die Daten auf beiden Mitgliedern doppelt vorhanden sind), können gespiegelte Datenträger kostenintensiv sein.

Achtung: Beim Löschen eines gespiegelten Datenträgers werden alle Informationen auf diesem Datenträger gelöscht.

Diskduplexing

Wenn beide physischen Laufwerke eines gespiegelten Datenträgers vom selben Controller gesteuert werden und der Controller ausfällt, kann auf kein Mitglied des gespiegelten Datenträgers zugegriffen werden. sie können einen zweiten Controller in den Computer einbauen, sodass jedes Laufwerk des gespiegelten Datenträgers über einen eigenen Controller verfügt. Diese Konfiguration, die Diskduplexing genannt wird, kann den gespiegelten Datenträger vor Controller- und Festplattenausfällen schützen. Verschiedene Hardwareimplementierungen von Diskduplexing verwenden auf einer einzelnen Festplattencontrollerkarte zwei oder mehrere Kanäle.

Durch Diskduplexing werden der Busverkehr reduziert und die Leseleistung u. U. gesteigert. Diskduplexing ist eine Hardwareerweiterung eines gespiegelten Windows 2000-Datenträgers, für die keine weitere Softwarekonfiguration erforderlich ist.

RAID 5-Datenträger

Windows 2000 Server unterstützt ferner die Fehlertoleranz mittels Stripesetdatenträgern mit Parität (RAID 5). Die Parität ist ein mathematisches Verfahren zur Bestimmung der Anzahl gerader und ungerader Bits in einem Wert oder einer Wertfolge, mit dem Daten rekonstruiert werden können, wenn ein Wert in einer Wertfolge verlogen gegangen ist.

Bei einem RAID 5-Datenträger erzieht Windows 2000 die Fehlertoleranz dadurch, dass jeder Laufwerkpartition des Datenträgers ein sog. Stripe mit Paritätsinformationen hinzugefügt wird (siehe Abbildung 12.12). Falls ein Laufwerk ausfällt, kann Windows 2000 die Daten und Paritätsinformationen auf den verbleibenden Laufwerken verwenden, um die Daten auf dem ausgefallenen Laufwerk zu rekonstruieren.

Aufgrund der Paritätsberechnung sind Schreibvorgänge auf einem RAID 5-Datenträger langsamer als auf einem gespiegelten Datenträger. RAID 5-Datenträger bieten jedoch eine bessere Leseleistung als gespiegelte Datenträger, insbesondere mit mehreren Controllern, da die Daten auf mehrere Laufwerke verteilt sind. Wenn hingegen ein Laufwerk ausfällt, verlangsamt sich die Leseleistung eines RAID 5-Datenträgers solange, bis Windows 2000 Server die Daten auf dem ausgefallenen Laufwerk mit Hilfe der Paritätsinformationen rekonstruiert hat.

RAID 5-Datenträger haben gegenüber gespiegelten Datenträgern einen Kostenvorteil, da die Speicherplatznutzung optimiert wird. Je mehr Laufwerke in einem RAID 5-Datenträger vorhanden sind, desto geringer sind die Kosten für den redundanten Datenstripe. Die folgende Tabelle zeigt, wie der für den Datenstripe benötigte Speicherplatz gesenkt wird, wenn dem RAID 5-Datenträger 2-GB-Festplatten hinzugefügt werden.

Anz.d. Laufwerke	Belegter Speicherplatz	Verfügbarer Speicherplatz	Redundanz
3	6 GB	4 GB	33 %
4	8 GB	6 GB	25 %
5	10 GB	8 GB	20 %

Bei Software-RAID 5-Datenträgern gelten folgende Einschränkungen. Erstens umfassen RAID-5-Datenträger mindestens drei und höchstens 32 Festplattenlaufwerke. Zweitens darf ein Software-RAID 5-Datenträger keine Start- oder Systempartition enthalten.

Für das Betriebssystem Windows 2000 stellen Hardware-RAID-Implementierungen keine Besonderheit dar. Aus diesem Grund gelten die Einschränkungen von Software-RAID-Konfigurationen nicht für Hardware-RAID-Konfigurationen.

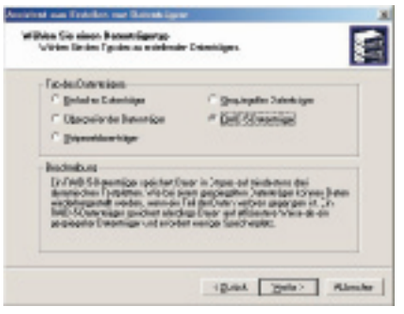
Gespiegelte und RAID 5-Datenträger – Vergleich

Gespiegelte und RAID 5-Datenträger bieten einen unterschiedlichen Grad an Fehlertoleranz. Die Auswahl der zu implementierenden Lösung hängt vom Grad des benötigten Schutzes und den Hardwarekosten ab. Die Hauptunterschiede zwischen gespiegelten Datenträgern (RAID 1) und RAID 5-Datenträgern liegen bei Leistung und Kosten. Die folgende Tabelle erklärt Unterschiede zwischen den Softwareimplementierungen von RAID 1 und RAID 5.

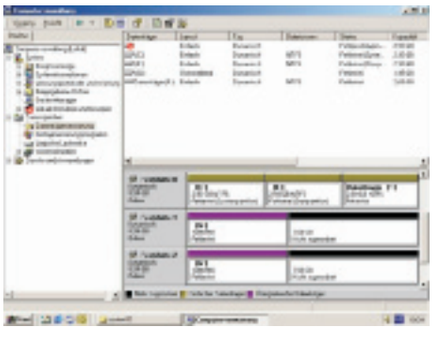
Gespiegelte Datenträger RAID 1	Stripesetdatenträger mit RAID 5
Unterstützen FAT und NTFS	Unterstützten FAT und NTFS
Können System- oder Startpartition schützen	Können System- oder Startpartition nicht schützen
Benötigen zwei Festplatten	Benötigen mindestens drei Festplatten und maximal 32 Festplatten
Höhere Kosten pro Megabyte	Niedrigere Kosten pro Megabyte
50 %-ige Speicherbelegung	Mindestens 33 %-ige Speicherbelegung
Gute Schreibleistung	Mittelmäßige Schreibleistung
Gute Leseleistung	Hervorragende Leseleistung
Benötigen weniger Systemspeicher	Benötigen mehr Systemspeicher

Gespiegelte Datenträger bieten in der Regel eine vergleichbare Lese- und Schreibleistung wie einzelfestplatten. RAID 5-Datenträger bieten jedoch eine bessere Leseleistung als gespiegelte Datenträger, insbesondere mit mehreren Controllern, da die Daten auf mehrere Laufwerke verteilt sind. Dadurch, dass die Paritätsinformationen berechnet werden müssen, wird jedoch mehr Arbeitsspeicher benötigt, wodurch sich die Schreibleistung verlangsamen kann.

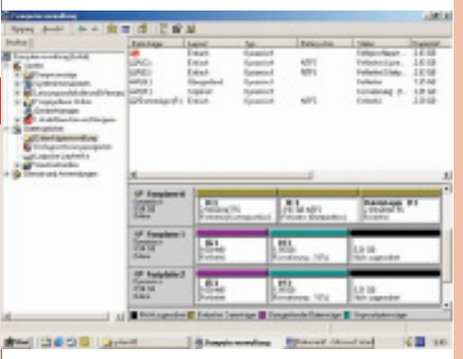
Gespiegelte Datenträger belegen nur 50 % des verfügbaren Speicherplatzes, weshalb die Kosten pro Megabyte (MB) höher sind als bei Laufwerken ohne Spiegelung. Bei Verwendung der Mindestanzahl an Festplatten (drei) belegen RAID 5-Datenträger 33% des verfügbaren Speicherplatzes mit Paritätsinformationen. Werden weitere Festplatten hinzugefügt, wird die Speicherplatzbelegung entsprechend gesenkt.



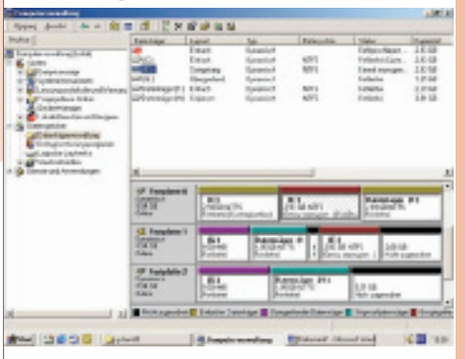
Beispiel: Übergreifender Datenträger = Partition, die auf zwei physische Festplatten verteilt ist (untere Abb: Laufwerk G:)



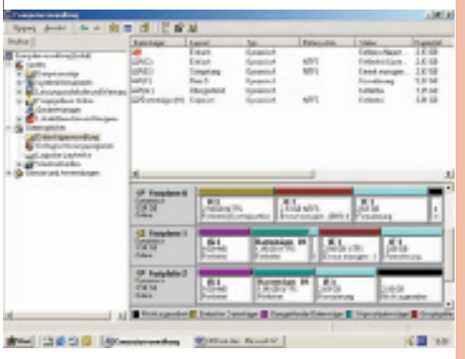
Beispiel: RAID 0 = Stripeset-Datenträger (Laufwerk H:)

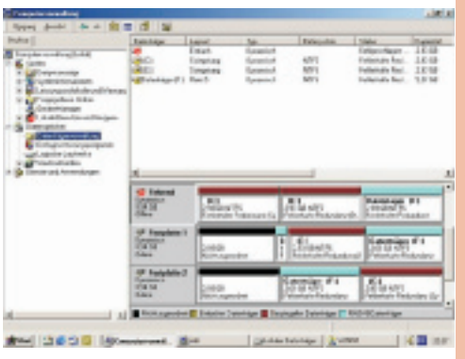


Beispiel: Gespiegelter Datenträger = RAID 1-Datenträger (Laufwerk E:)



Beispiel: RAID 5-Datenträger (Laufwerk F:)





Windows Vista-Sicherheitseinstellungen

In Windows Vista wurden eine Reihe zusätzlicher Sicherheitskonfigurationen eingeführt. Die mit Windows XP SP2 eingeführten Maßnahmen wurden oft erheblich erweitert und verbessert.

Sicherheitscenter

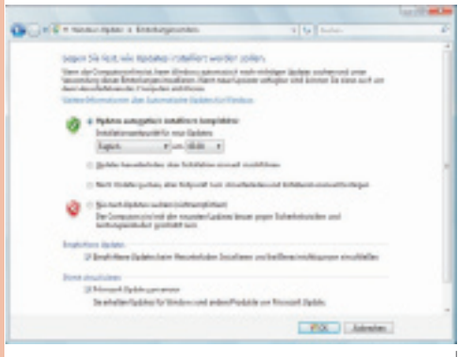
Damit lassen sich maßgebliche Sicherheitseinstellungen bequem verwalten:

- Windows Update
- Windows-Firewall
- Windows-Defender
- Internetoptionen

Windows Update

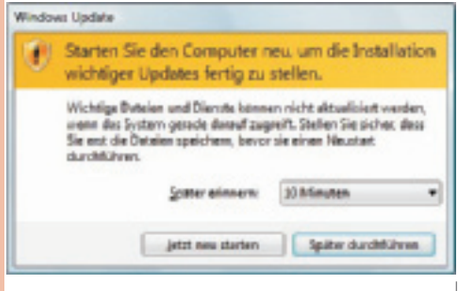
Windows Update sorgt durch die Bereitstellung von Microsoft Windows Vista-Softwareupdates dafür, dass Ihr Computer sicherheitstechnisch auf dem neuesten Stand bleibt. Sie können Windows Update so konfigurieren, dass Updates automatisch heruntergeladen und installiert werden. Sie müssen dieses Feature lediglich aktivieren und brauchen sich anschließend nicht mehr darum zu kümmern.

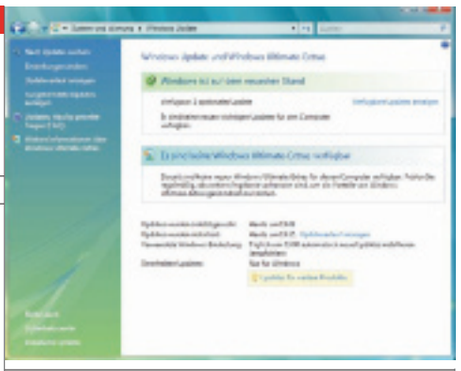
Updates beinhalten Fehlerkorrekturen, Sicherheitspatches und Verbesserungen und sollten daher regelmäßig eingespielt werden.



Unter Windows Vista geht der Funktionsumfang von Windows Update über den von Windows XP gebotenen Funktionsumfang hinaus, wodurch Updates einfacher und störungsfreier erfolgen.

Eine Anpassung der Einstellungen und Aktionen von Windows Update ermöglicht reibungslose Updates und bietet Flexibilität, sobald diese Updates bereitstehen.





Windows Firewall

Die Windows Vista-Firewall sorgt für einen Schutz vor Hackern, Viren und Würmern, die versuchen, aus dem Internet auf Ihren Computer zu gelangen.

Eine Firewall trägt zur Sicherheit des Computers bei. Sie schränkt die Übertragung von Informationen, die von anderen Computern bei Ihrem Computer eingehen, ein, so dass Sie eine bessere Kontrolle über die Daten auf Ihrem Computer haben und besser vor Personen oder Programmen (einschließlich Viren und Würmer) geschützt sind, die unaufgefordert versuchen, eine Verbindung mit Ihrem Computer herzustellen.

Sie können sich eine Firewall wie eine Absperrung vorstellen, die die Daten (häufig auch Verkehr genannt), die aus dem Internet oder einem Netzwerk eingehen, überprüft und diese Daten dann in Abhängigkeit von den Firewalleinstellungen entweder zurückweist oder zum Computer passieren lässt.

In Microsoft Windows Vista ist die Windows-Firewall standardmäßig aktiviert. (Möglicherweise wird sie jedoch von einigen Computerherstellern und Netzwerkadministratoren deaktiviert.) Es ist nicht nötig, die Windows-Firewall zu verwenden; Sie können jeden gewünschten Firewall installieren und ausführen. Informieren Sie sich über die Features anderer Firewalls, und entscheiden Sie dann, welcher Firewall Ihre Anforderungen am besten erfüllt. Wenn Sie sich für die Installation und Ausführung einer anderen Firewall entscheiden, sollten Sie die Windows-Firewall deaktivieren.

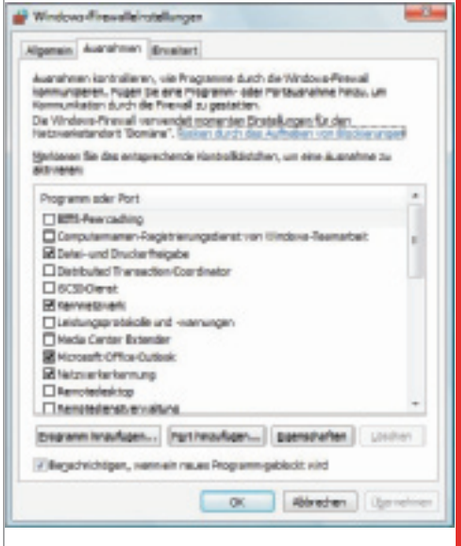
Funktionsweise: Wenn ein Benutzer im Internet oder in einem Netzwerk versucht, eine Verbindung mit Ihrem Computer herzustellen, sprechen wir bei diesem Versuch von einer "unverlangten Anforderung". Wenn eine unverlangte Anforderungen bei Ihrem Computer eingeht, wird die Verbindung von der Windows-Firewall gesperrt. Wenn Sie ein Programm ausführen, z. B. ein Instant Messaging-Programm oder ein Multiplayer-Netzwerkspiel, das auf den Empfang von Daten aus dem Internet oder einem Netzwerk angewiesen ist, werden Sie von der Firewall gefragt, ob die Verbindung gesperrt bleiben oder die Sperrung aufgehoben (d. h. die Verbindung zugelassen) werden soll. Wenn Sie die Sperrung der Verbindung aufheben, erstellt der Windows-Firewall eine Ausnahme, so dass sich der Firewall in Zukunft nicht mehr daran stört, wenn dieses Programm Daten empfangen muss.

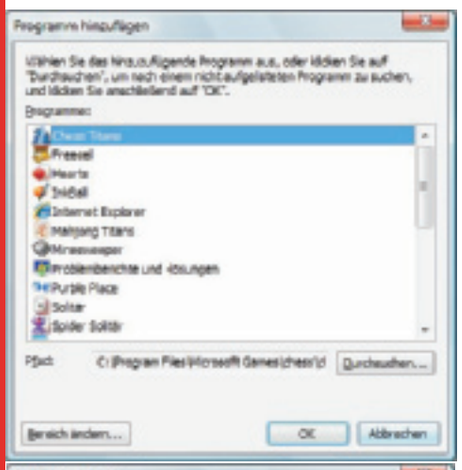
Wenn Sie beispielsweise Sofortnachrichten mit einer anderen Person austauschen, die Ihnen eine Datei (z. B. ein Foto) senden möchte, werden Sie vom Windows-Firewall gefragt, ob Sie die Sperrung für die Verbindung aufheben und den Empfang des Fotos auf Ihrem Computer zulassen möchten. Wenn Sie zusammen mit Freunden ein Multiplayerspiel über das Internet spielen möchten, können Sie das Spiel ebenfalls als Ausnahme hinzufügen, so dass der Firewall den Empfang der Spieledaten auf Ihrem Computer zulässt.

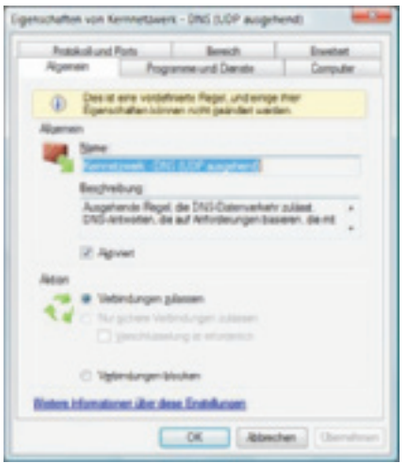
Sie können die Windows-Firewall zwar für bestimmte Internet- und Netzwerkverbindungen deaktivieren, allerdings erhöhen Sie damit das Risiko, dass die Sicherheit des Computers beeinträchtigt wird.

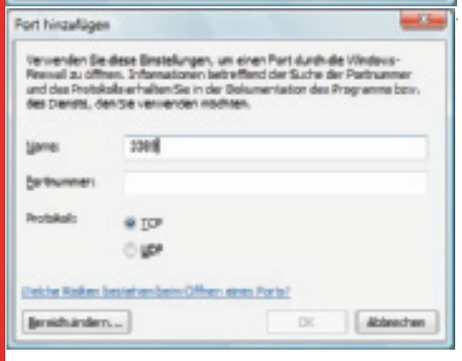
Konfiguration der Windows Firewall

Eigenschaften der LAN-Verbindung oder Systemsteuerung



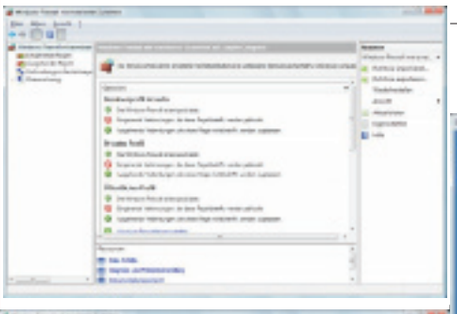


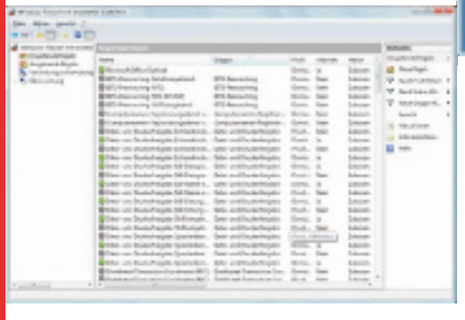




Erweiterte Firewall-Konfiguration

Weitere Details können im Verwaltungsmenü unter „Windows-Firewall mit erweiterter Sicherheit" konfiguriert werden:





Beispiele für benötigte Ports:

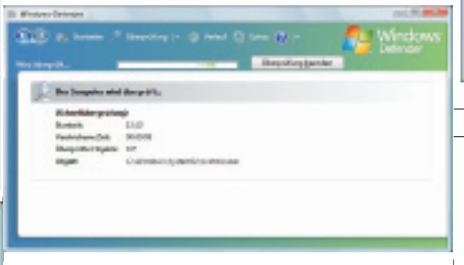
Datei- und Druckerfreigabe: TCP 139, 445, UDP 137, 138

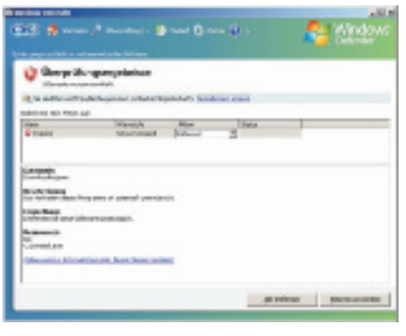
Remote-Desktop: 3389

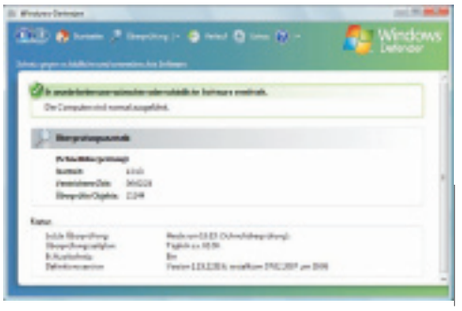
VPN: 1723

Windows Defender

Der Windows-Defender schützt Sie vor Spyware und anderer möglicherweise unerwünschter Software.

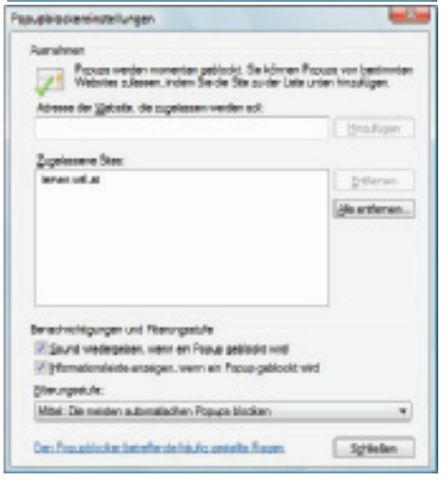






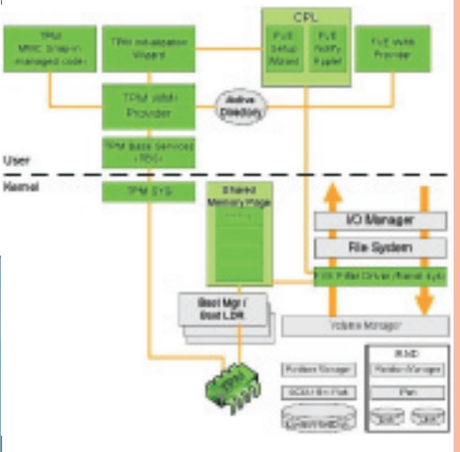
Popup-Blocker

Im Internet Explorer 7 ist der Popup-Blocker standardmäßig aktiviert:



BitLocker

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. Das optionale Feature verschlüsselt auf Wunsch die verfügbaren Festplatten. Dabei ist der Schutz bereits während des Bootvorgangs aktiv.



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.

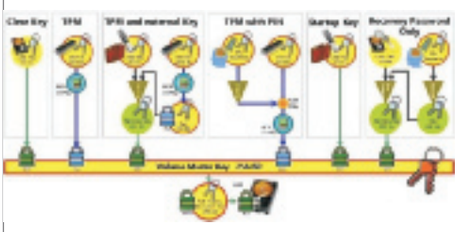
Zutritt verweigert: Nur wenn alle digitalen Schlüssel passen, werden die Daten entschlüsselt. (Quelle: Microsoft)

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 angegebene 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.

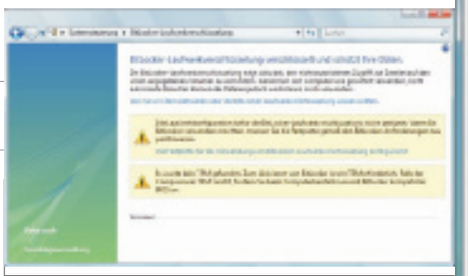


Schlüsselbrett: Der Volume Master Key dient als zentraler Zugangsschlüssel. (Quelle: Microsoft)

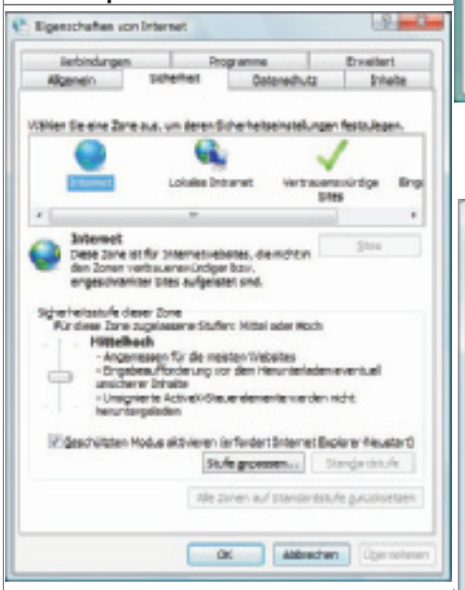
Aus dem VMK schließlich werden alle Schlüsselwerte für den Nutzer und die Recovery-Optionen erstellt. Löscht man also einen kompromittierten VMK, haben alle damit erstellten Schlüssel keinen Zugriff mehr.

IT-Administratoren können BitLocker künftig wahlweise lokal oder per Remote-Zugriff kontrollieren. Neben der Management-Funktion gibt es verschiedene Assistenten und Scripts.

Die konkrete Konfiguration kann über die Systemsteuerung erfolgen; zum optimalen Einstellen des Schutzes ist aber bereits ein spezieller Betriebssystem-Installationsvorgang erforderlich.



Internet-Optionen



Windows-Tool zum Entfernen bösartiger Software

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

Virenschutzlösungen

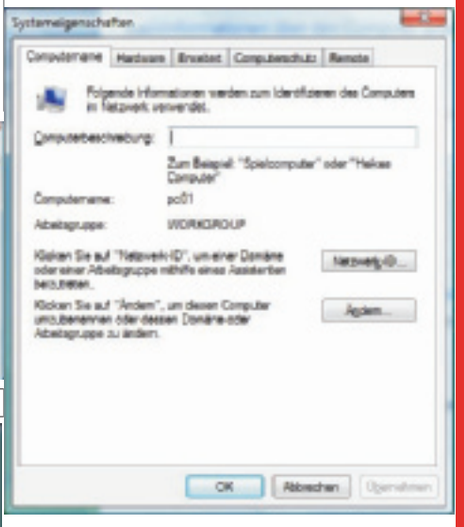
Zusätzlich zu diesen integrierten Windows Vista-Features sollten Sie auf dem Computer eine Virenschutzsoftware wie Windows OneCare oder eine Virenschutzlösung eines Partners von Microsoft aktivieren. Unabhängig von der gewählten Lösung müssen Sie Ihre Virenschutzsoftware regelmäßig aktualisieren. Diese Aktualisierungen werden von den meisten Herstellern von Virenschutzsoftware als Abonnements bereitgestellt.

Im Zusammenspiel können diese Tools Ihren PC vor bösartiger Software schützen.

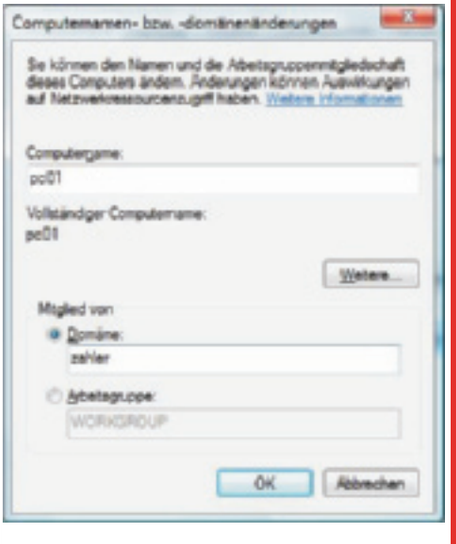
Aufnehmen von Arbeitsstationen in Active Directory-Domänen

Schritt 1 (WICHTIG!): Ändern Sie die IP-Konfiguration der Arbeitsstation so, dass als bevorzugter DNS-Server die IP-Adresse des Domänencontrollers eingestellt wird. (Wir nehmen an, dass der Domänencontroller selbst der für die Domäne zuständige DNS-Server ist.)

Schritt 2: Öffnen Sie die ***Systemeigenschaften*** (***Systemsteuerung*** – System oder Tastenkombination ***Windows-Pause***) und zeigen Sie das Dialogfeld ***„Computername"*** an. Dort klicken Sie auf die Schaltfläche ***„Ändern"***:

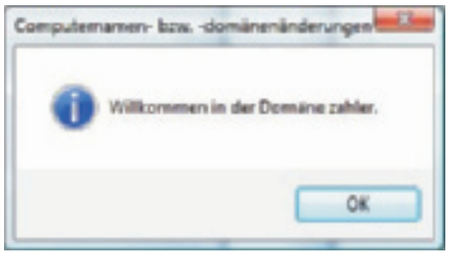


Ändern Sie im folgenden Dialogfeld die Einstellung ***„Mitglied von"*** auf ***„Domäne"*** und geben Sie den NetBIOS-Namen der Domäne an.

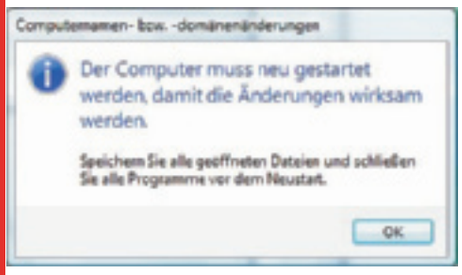


Sie werden nun nach einem Konto gefragt, das in der Lage ist, Computerkonten zum Active Directory hinzuzufügen. Geben Sie hier die Anmeldeinformationen des **Domänenadministrators** an.

Nach einiger Zeit wird der Vorgang mit der Erfolgsmeldung *„Willkommen in der Domäne Domänenname"* bestätigt.



Abschließend muss der Computer neu gestartet werden.



Vorgänge beim Aufnehmen eines Computers in die Domäne:

- Im Active Directory wird ein Computerkonto erzeugt.
- In der AD-integrierten DNS-Zone der Domäne wird ein A-Eintrag (und gegebenenfalls auch ein PTR-Eintrag) für den Computer erzeugt.
- Am Arbeitsstations-PC wird die Sicherheitsgruppe *„Domänen-Admins"* zur lokalen Gruppe *„Administratoren"* hinzugefügt.
- Am Arbeitsstations-PC wird die Sicherheitsgruppe *„Domänen-Benutzer"* zur lokalen Gruppe *„Benutzer"* hinzugefügt. (Überlegen Sie: Warum?)

Vista und mobile Geräte

Windows Vista bietet spezielle Unterstützung für mobile Geräte. Zu den mobilen Geräten gehören:

- Notebooks
- Tablet PCs
- PDAs, vorzugsweise mit Windows Mobile V6

Windows-Mobilitätscenter

Mit dem Windows-Mobilitätscenter können Sie an einem zentralen Ort schnell auf die Einstellungen Ihres mobilen PCs zugreifen. Sie können beispielsweise die Lautsprecherlautstärke Ihres mobilen PCs anpassen, den Status Ihrer drahtlosen Netzwerkverbindung überprüfen und die Helligkeit des Bildschirms anpassen – alles an einem zentralen Ort.

Sie müssen sich nicht mehr merken, wo sich Einstellungen in der Systemsteuerung befinden. Dies ist insbesondere dann hilfreich, wenn Sie Einstellungen schnell anpassen müssen, um Ihren mobilen PC an unterschiedlichen Orten zu verwenden, zum Beispiel auf dem Weg von Ihrem Schreibtisch in eine Besprechung oder auf dem Weg vom Flughafen nach Hause. Dadurch, dass Sie diese Einstellungen zentral anpassen können, sparen Sie Zeit, ganz gleich, ob Sie Ihren mobilen PC für geschäftliche oder private Zwecke verwenden.

Sie können das Mobilitätscenter mit einer der folgenden Methoden öffnen:

- Klicken Sie auf die Schaltfläche *Start*, klicken Sie auf *Systemsteuerung*, klicken Sie auf *Mobil-PC*, und klicken Sie dann auf *Windows-Mobilitätscenter*.
- Klicken Sie auf das Symbol für die *Akkumessanzeige* im Infobereich der Windows-Taskleiste, und klicken Sie dann auf *Windows-Mobilitätscenter*.
- Drücken Sie Windows-Logo-Taste + X.

Das Mobilitätscenter besteht aus mehreren der am häufigsten verwendeten mobilen PC-Einstellungen. Je nach System weist das Fenster des Mobilitätscenters einige, möglicherweise jedoch nicht alle der folgenden Kacheln auf:

- **Helligkeit**. Ziehen Sie den Schieberegler, um die Helligkeit der Anzeige vorübergehend anzupassen. Um die Helligkeitseinstellungen des Bildschirms für Ihren Energiesparplan anzupassen, klicken Sie auf das Symbol auf der Kachel, um Energieoptionen in der Systemsteuerung zu öffnen.
- **Lautstärke**. Ziehen Sie den Schieberegler, um die Lautsprecherlautstärke des mobilen PCs anzupassen, oder aktivieren Sie das Kontrollkästchen *Ton aus*.
- **Akkustatus**. Zeigen Sie die Restkapazität des Akkus an, oder wählen Sie aus einer Liste einen Energiesparplan aus.
- **Drahtlosnetzwerk**. Zeigen Sie den Status der Drahtlosnetzwerkverbindung an, oder schalten Sie den Drahtlosnetzwerkadapter ein oder aus.
- **Bildschirmausrichtung**. Ändern Sie die Ausrichtung des Bildschirms des Tablet PCs von Hochformat in Querformat und umgekehrt.
- **Externer Bildschirm**. Schließen Sie einen zusätzlichen Monitor am mobilen PC an, oder passen Sie die Anzeigeeinstellungen an.
- **Synchronisierungscenter**. Zeigen Sie den Status einer laufenden Dateisynchronisierung an, starten Sie eine neue Synchronisierung, und passen Sie die Einstellungen im Synchronisierungscenter an.
- **Präsentationseinstellungen**. Passen Sie Einstellungen wie die Lautsprecherlautstärke und das Desktophintergrundbild an, um eine Präsentation zu halten.

Wenn Sie weitere Anpassungen an den Einstellungen Ihres mobilen PCs vornehmen müssen, für die Sie auf die Systemsteuerung zugreifen müssen, klicken Sie auf das Symbol auf einer Kachel, um die Systemsteuerung für diese Einstellungen zu öffnen. Sie können beispielsweise einen vorhandenen Energiesparplan aus der Kachel Akkustatus auswählen, oder Sie können auf das Symbol auf der Kachel klicken, um zum Erstellen eines Energiesparplans Energieoptionen in der Systemsteuerung zu öffnen.

Hinweise

- Einige Kacheln im Mobilitätscenter wurden vom Hersteller Ihres mobilen PCs hinzugefügt. Weitere Informationen hierzu finden Sie in der Begleitdokumentation zu Ihrem mobilen PC oder auf der Website des Herstellers.
- Wenn eine Kachel nicht angezeigt wird, kann dies daran liegen, dass die erforderliche Hardware, z. B. ein Drahtlosnetzwerkadapter, oder die erforderlichen Treiber fehlen.

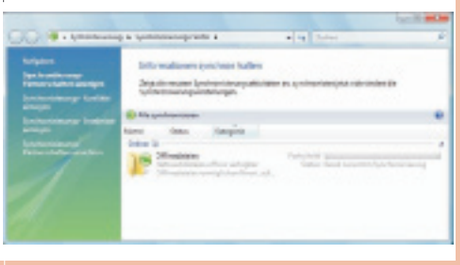
Synchronisierungscenter

In Windows bezeichnet Synchronisierung den Vorgang, Dateien an zwei oder mehr Orten identisch zu halten.

Die Synchronisierung kann unidirektional oder bidirektional erfolgen. Bei der unidirektionalen Synchronisierung werden jedes Mal, wenn Sie eine Datei oder andere Informationen an einem Ort hinzufügen, ändern oder löschen, dieselben Informationen am anderen Ort hinzugefügt, geändert oder gelöscht. Es werden jedoch nie Änderungen am ersten Ort ausgeführt, da die Synchronisierung nur in einer Richtung erfolgt.

Bei der bidirektionalen Synchronisierung werden Dateien in beide Richtungen kopiert, um die Dateien an beiden Orten synchron zu halten. Jedes Mal, wenn Sie eine Datei an einem Ort hinzufügen, ändern oder löschen, wird dieselbe Änderung am anderen Ort ausgeführt. Es spielt keine Rolle, ob Sie die Änderungen auf einem Computer, einem mobilen Gerät oder in einem Ordner auf einem Netzwerkserver vorgenommen haben. Dieselben Änderungen an beiden Orten ausgeführt. Die bidirektionale Synchronisierung wird meist in Arbeitsumgebungen verwendet, in denen Dateien häufig an mehreren Orten aktualisiert und dann mit anderen Orten synchronisiert werden.

Im Synchronisierungscenter können Sie den Computer mit Netzwerkordnern, mobilen Geräten und kompatiblen Programmen synchronisieren. Das Synchronisierungscenter kann Dateien und Ordner an verschiedenen Orten automatisch synchron halten.



http://www.microsoft.com/windows/products/windowsvista/

Fehleranalyse in Windows (Vista)

oder „In 18 (einfachen) Schritten Computerprobleme lösen"

Christian Haberl

Eines vorweg: Ich versuche hier eine möglichst vollständige Liste der Schritte zu erstellen, die ich durchführe, wenn ich ein Problem, z.B. mit einem System das häufig abstürzt, lösen möchte. Es ist aber weder notwendig, alle Schritte durchzuführen, noch muss es exakt diese Reihenfolge sein.

Wenn es einem nichts ausmacht, neu zu installieren, kann genau das zum Beispiel der erste Schritt sein, oder man schaut sich gleich den *Crash Dump* an. Oder man hat vielleicht schon eine Vermutung in Richtung Hardware (Speicher, Festplatte, Überhitzung...) dann kann man dort beginnen.

Ich möchte auf den meisten meiner Systeme Neuinstallationen vermeiden, weil Dutzende Programme drauf installiert sind, die Konfiguration teils monate- oder jahrelang gewachsen, gepflegt und auf meine Bedürfnisse angepasst ist. Zugegeben: Bei Mac OS wäre das alles einfacher, da lassen sich installierte Programme leichter auf eine Neuinstallation migrieren. Aber das ist ein anderes Thema.

Ich jedenfalls versuche, Neuinstallationen so gut wie möglich zu vermeiden und komme mit einem oder mehreren der folgenden Schritte eigentlich immer ganz gut zum Ziel.

Mein Tipp daher, die Liste zunächst von Anfang bis Ende durchlesen, und dann eine eigene Reihenfolge oder Gewichtung erstellen.

Außerdem sei noch erwähnt, dass Vieles hier auch für ältere Windows Versionen gilt, beziehungsweise sogar betriebssystemunabhängig nützlich sein kann. Manche Dinge, die das Troubleshooting erleichtern, gibt es aber erst in Windows Vista (Problemberichte und Lösungen, Zuverlässigkeitsüberwachung, Speicherdiagnosetool...)

Für den folgenden Beitrag muss man zwar kein Techniker sein, manche technische Grundbegriffe wie „*Registry*" sollte man aber beherrschen. Wenn einzelne Tipps nicht verständlich sind, sollte man lieber die Finger davon lassen, um nicht eventuell mehr Schaden anzurichten, als man behebt.

1 Nachdenken / Nachgoogeln

Also, der erste Schritt ist einmal: Nachdenken und Nachgoogeln. Zum Beispiel bei einem Bluescreen mit "`dne2000.sys`" ist recht schnell der Übeltäter gefunden. Google verrät, dass diese Komponente wohl was mit einer VPN Client Software zu tun hat. Von Cisco, Sonicwall oder anderen Herstellern. BAM! - Problem gefunden, da musste ich doch kürzlich bei einem Kunden einen Sonicwall VPN Client installieren um in's WLan zu kommen (?!) - was für ein Unsinn eigentlich. - Weg mit dem Mist, Problem gelöst.

(Eigentlich ärgerlich dass Hersteller, die sich auf Sicherheit spezialisieren, nicht einmal stabile Software machen können, dieses `dne2000.sys` macht wohl schon seit Windows 2000 laufend Probleme, wenn man sich durch das Thema durchgoogelt.)

2 Problemberichte und -lösungen

Nur Windows Vista

Problemberichte- und Lösungen hilft bei der Lösung von Hardware- und Softwareproblemen in dem es manuell oder automatisch Fehlerberichte an Microsoft sendet. Ist zu einem Fehler schon eine Lösung bekannt, bekommt man umgehend die Lösung angezeigt.

Dazu ein kleines Beispiel aus meinem Alltag: Im Rahmen meiner Tätigkeit als Trainer für die CC | Akademie habe ich für ein Training zehn PCs mit Windows Vista samt Treibern und Software vorbereitet. Der erste Teilnehmer schaltet seinen PC ein – Bluescreen. Peinlich. Was war passiert? Ich hatte einen falschen Grafikkartentreiber installiert gehabt (bzw. genau gesagt wurden kurzfristig andere Grafikkarten für die Trai-

ningsrechner angekauft…) Mir ging durch den Kopf: „Wie überspiele ich das jetzt? Wie kann ich so tun als wäre das ein Teil des Trainings?"

Ich riskierte es: Nach einem Neustart forderte ich den Teilnehmer auf, den Fehler an Microsoft zu melden. Ohne meine Aufforderung hätte er das glatt weggeklickt.

Ich hatte Glück: Nur Sekunden nach dem Senden des Problemberichts kam die Lösung zurück: *„Problem verursacht durch Grafikkartentreiber, laden Sie hier den richtigen Treiber herunter…"* – Während ich die Lösung und dieses Feature noch erklärte flackerte der Bildschirm kurz, Windows Update hatte im Hintergrund schon den Treiber aktualisiert. Problem behoben!

Also: Problemberichte unbedingt senden, am besten automatisch. Es kommen verdammt oft brauchbare Lösungen zurück, manchmal blitzschnell. Persönliche Daten werden nicht an Microsoft übermittelt. Außerdem hilft man Microsoft damit Software- und Treiberprobleme rasch an den verantwortlichen Hersteller zu melden, sodass dieser den Fehler rasch beheben kann. Sobald dieser Fehler behoben ist, liefert das Feature „Problemberichte und –lösungen" die Lösung zurück, meistens gleich direkt mit Downloadlink, so wie in dieser Abbildung.

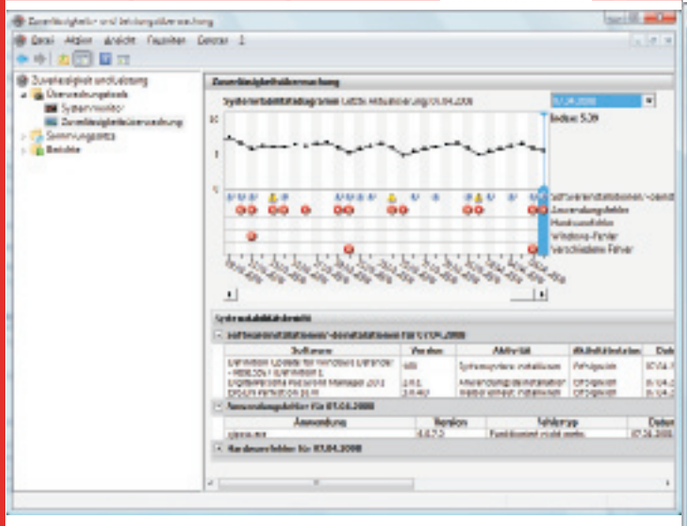
Als Firma kann man übrigens auch einen firmeninternen Reporting Server zwischenschalten, wenn man nicht will, dass jeder Benutzer Fehler direkt an Microsoft berichtet. Dieses Feature nennt sich dann *„Corporate Error Reporting"* bzw. *„Desktop Error Reporting"*.

Besonders ausführlich beschreibt Kay Giza das Feature „Problemberichte und -lösungen" in seinem Blog:

`http://www.giza-blog.de/WasIstAusDrWatsonGewordenNaProblemberichteUndLoesungenVista.aspx`

3 Zuverlässigkeitsüberwachung

Nur Windows Vista

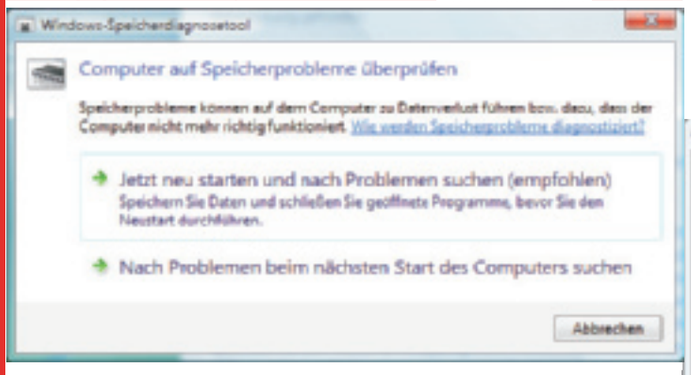


Eines der wichtigsten Troubleshooting Werkzeuge überhaupt in Windows Vista, die *„Zuverlässigkeitsüberwachung"* eignet sich besonders gut für wiederkehrende Probleme, aber auch für das Aufspüren kausaler Zusammenhänge.

Es stellt auf einer Zeitachse die Systemstabilität (0-10) dar. Dieses Systemstabilitätsdiagramm zeigt jeweils in einer eigenen Zeile *„Software(de)installationen"* und Fehler von den Typen *„Anwendungsfehler"*, *„Hardwarefehler"*, *„Windows-Fehler"* und *„Verschiedene Fehler"* – So kann man rasch erkennen, welche z.B. Treiberinstallation einem regelmäßig auftretenden Problem vorausging.

4 Hauptspeicher (Memory)

Nur Windows Vista



Windows Vista enthält ein Speicherdiagnosetool (`mdsched.exe`), das die Speicherbausteine auf Herz und Nieren prüft.

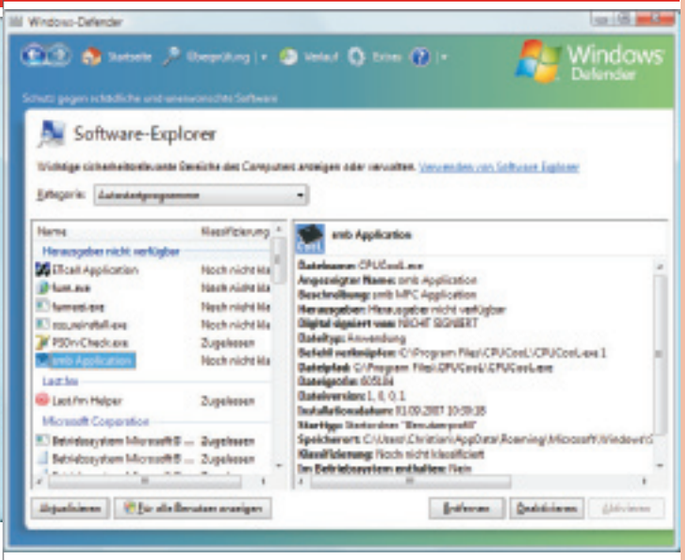
Hat man zwei oder mehr Speicherriegel verbaut, sollte man überdies testen, ob es mit nur je einem der beiden die Probleme vielleicht nicht gibt.

Ich hatte z.B. einmal ein System, da war wohl am Mainboard etwas defekt, was dazu geführt hat, dass Speicherfehler auftraten, aber nur wenn zwei Speicher-Riegel verbaut waren. Mit einem lief das System einwandfrei, egal mit welchem der beiden.

Also Vorsicht: Nicht nach fehlgeschlagener Speicherprüfung gleich neuen Speicher kaufen!

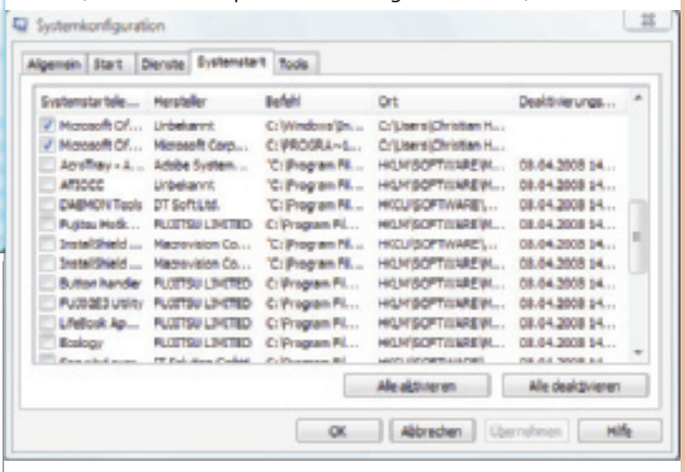
Wenn aber alle Speicherbausteine, auch bei separater Prüfung zu Fehlern beim Speicherdiagnosetool führen, liegt hier der Übeltäter!

5 Dienste und Autostartprogramme

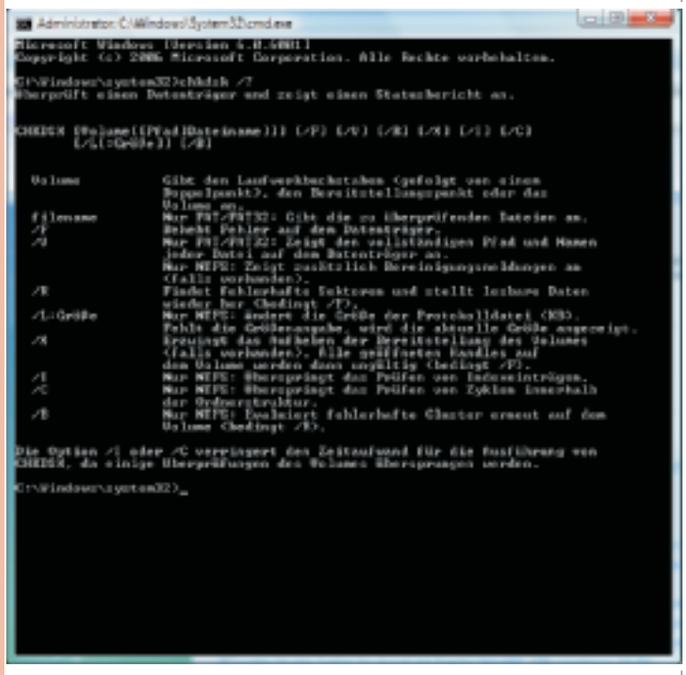


`msconfig.exe` oder der Software-Explorer in **Windows Defender** erlauben es, gezielt Dienste und Autostartprogramme, die man vielleicht im Verdacht hat, das System zu destabilisieren zu deaktivieren. Der Software-Explorer ist ein Teil von Windows Defender und befindet sich unter Extras, er erlaubt es nicht nur, Autostartprogramme zu deaktivieren, sondern sogar diese zu entfernen, und dabei ist es egal wie sich dieses Autostartprogramm in das System hineinhängt - der Ordner *Autostart* im *Startmenü* ist nur mehr einer der vielen Wege, ein Programm nach dem Systemstart automatisch auszuführen. Ein weiterer Weg ist ein Eintrag in der Registry etwa unter `Software\Microsoft\Windows\CurrentVersion\Run` aber das sind noch lange nicht alle.

Sollten sich bestimmte Programme über Software-Explorer oder `msconfig` nicht abdrehen lassen (bei mir sind das z.B. iTunes und Quicktime), dann kann man auch direkt in die Registry reingehen und die entsprechenden Schlüssel unter `Software\Microsoft\Windows\CurrentVersion\Run` entfernen (eventuell vorher sichern, wenn man sie später wieder reingeben möchte).

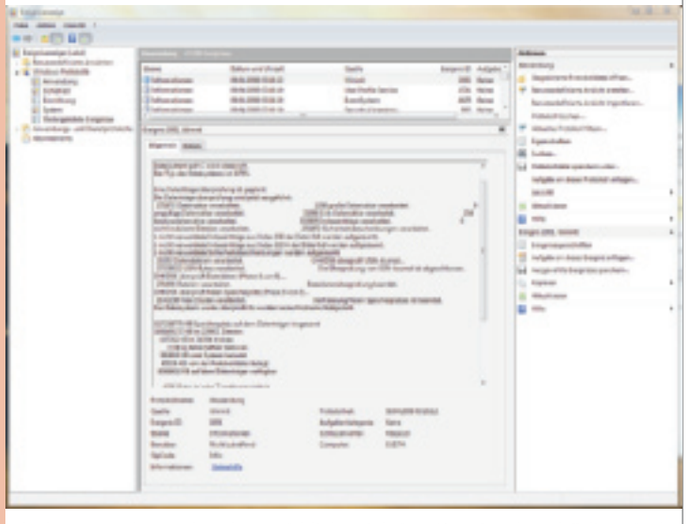


6 Festplatte



Der Befehl **chkdsk /f /r** versucht, Fehler auf der Festplatte und im Dateisystem zu beheben. Ein Durchlauf kann aber mehrere Stunden dauern, weshalb man das gerne über Nacht machen will. Außerdem muss man - wenn man die Systemplatte überprüfen will - den Computer neu starten. Doch wenn man dann am nächsten Tag wissen möchte, was das Ergebnis von **chkdsk** ist, ist Windows bereits hochgefahren, und **chkdsk** nicht mehr am Bildschirm, daher mein Tipp: Im ***Wininit***-Event der Anwendungs-Ereignisanzeige (Vista) wird protokolliert, was **chkdsk** gefunden bzw. gemacht hat, wenn es beim Booten ausgeführt wurde. (Unter XP war es noch das ***Winlogon***-Event)

Nun kann es sein, dass entweder kleinere Probleme im Dateisystem behoben wurden, oder dass wirklich wichtige Dateien beschädigt sind, oder aber dass die Festplatte tatsächlich physisch beschädigt ist. Im ersten Fall braucht man nichts weiter unternehmen. Im zweiten Fall sollte man sichergehen, dass man die eventuell beschädigten Dateien austauscht (siehe Punkt ***Systemdateien***) bzw. wenn eine Datei, die zu einem Treiber gehört, beschädigt wurde, dass man diesen Treiber neu installiert. Im letzten Fall, wenn sich also wirklich physisch beschädigte Sektoren auf der Festplatte häufen, sollte man die Festplatte rasch austauschen. Es droht weitere Instabilität des Systems und Datenverlust.

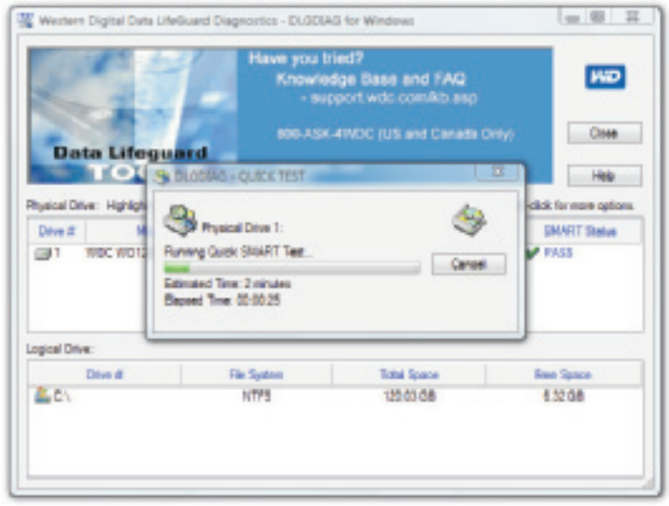


Im Fall eines Sturzes sollen Daten auf der Festplatte so besser vor einem Headcrash geschützt werden, indem der Schreib-Lesekopf während des Falls auf der "Rampe" positioniert wird, um den Aufschlag des Kopfes auf das Medium zu verhindern.

Neben **chkdsk** kann man auch die Tools der jeweiligen Festplatten-Hersteller verwenden, wo man genauere und zuverlässigere Informationen über die Festplatte bekommt.

Hier eine Übersicht über die Tools der Hersteller:

- Fujitsu *http://www.fel.fujitsu.com/home/drivers.asp*
  - FJDT (Fujitsu ATA Diagnostic Tool)
  - SDIAG (SCSI/SAS Diagnostic Tool)
- Hitachi/IBM *http://www.hitachigst.com/hdd/support/download.htm*
  - DFT - Drive Fitness Test (angeblich auch für Platten anderer Hersteller)
  - OGT Diagnostic Tool
- Seagate/Maxtor/Quantum
  http://www.seagate.com/www/en-us/support/downloads/
  - Seatools (Ersetzt auch Maxtor's Powermax Tool)
- Samsung
  http://www.samsung.com/global/business/hdd/support/utilities/Support_HUTIL.html
  - ESTool/HUTIL/SUTIL (The Drive Diagnostic Utility)
  - SHDIAG
- Toshiba
  - Kein eigenes Diagnose-Tool!
- Western Digital *http://support.wdc.com/download/*
  - Data Lifeguard Tools/Diagnostic



Tipp: Wenn (gerade bei Notebooks) die Festplatte als Fehlerquelle reduziert werden soll, kann man zu *Solid State Disks* greifen (sehr teuer) oder eine Festplatte mit *Free Fall Sensor* (*Shock Sensor*) verwenden.

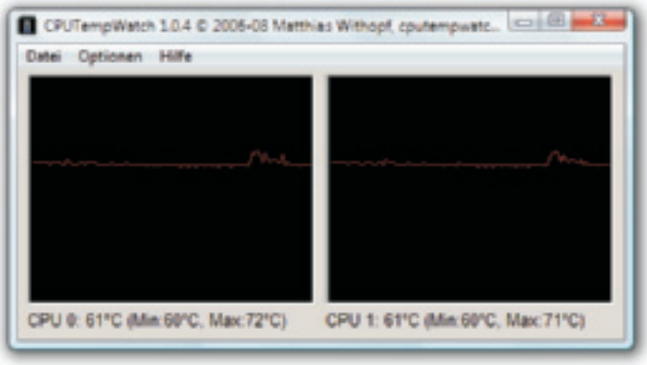
Zuletzt noch ein Tipp: Ist die Festplatte wirklich schuld und muss diese ersetzt werden, nicht vergessen, die Daten zu zerstören!

Aber bevor man diese aus dem Flugzeug wirft, auf die Straßenbahnschienen legt oder am Schießstand als Zielscheibe verwendet, kann man – wenn sie sich per Software noch ansprechen lässt – mit dem in Windows Vista enthaltenen Tool **cipher.exe** die Daten „shreddern" also unlesbar machen:

```
FORMAT drive_letter: /FS:NTFS /V:label /X
CIPHER /W:drive_letter:\
```

Die Festplatte wird damit in 3 Schritten zuerst mit Nullen, dann mit Einsen, dann mit Zufallswerten überschrieben. Wenn man ganz sicher gehen will, kann man das auch mehrfach ausführen.

7 Thermik / Überhitzung



Ausgefallene Lüfter, unzureichender Luftstrom oder Übertaktung führen oft zur Überhitzung von Systemkomponenten oder gar der CPU, was zu Abstürzen oder "Not-Abschaltungen" der CPU führen kann.

Gute Belüftung sicherstellen, Standgeräte sollten frei stehen, nicht eingezwängt zwischen Möbeln und schon gar nicht in der Nähe von Heizkörpern.

Lüfter - auch bei Notebooks - sollten regelmäßig von Staub befreit werden, weil sie sonst möglicherweise nicht mehr ordentlich kühlen oder „hängen bleiben". Die regelmäßigen Bluescreens in letzter Zeit auf meinem Notebook waren laut Fujitsu Siemens Service Techniker genau darauf zurückzuführen. Bei Lifebooks gibt es sogar einen Filter, den man abschrauben und reinigen kann, bzw. mit Druckluftspray dann sogar den Lüfter durchblasen kann/soll, wenn das Filterteil herausgeschraubt ist.

Um die Temperatur der Prozessoren zu überwachen, empfiehlt sich das kostenlose Tool **cputempwatch** von Matthias Withopf. *http://www.withopf.com/tools/cputempwatch/*

8 Steckkontakte

Gerade bei Standgeräten (Desktops) können nicht ordentlich sitzende Steckkarten oft zu Problemen führen. Diese überprüfen, gegebenenfalls ausbauen und neu einstecken.

9 „Crash Dump" analysieren

Jetzt geht's an's Eingemachte. Die Hardware (Festplatte und Speicher) ist es nicht, die Bluescreens spucken vielleicht den Übeltäter nicht eindeutig aus, Problemberichte- und Lösungen und Zuverlässigkeitsüberwachung in Vista geben keine Anhaltspunkte? - Dann ran an den Crashdump!

Bluescreens haben etwas ziemlich Mystisches an sich. Viele Anwender meinen, dass es Stop-Fehler nur unter Windows gibt, und diese etwas mit der (fehlenden) Stabilität des Betriebssystems selbst zu tun haben.

Wer sich über Microsoft und/oder Windows lustig machen möchte, erwähnt gerne gehässigt diese *Bluescreens of Death* (BSOD) und ihre angebliche Häufigkeit unter Windows Betriebssystemen.

Man könnte dann kontern, dass in anderen Betriebssystemen ein Bluescreen gar nicht auffällt, weil er sich von der Benutzeroberfläche kaum unterscheidet ;-)

Tatsächlich gab es aber vor allem zur Zeit von Windows 98 und Windows ME noch sehr viele Bluescreens.

Heute - also unter NT basierten Betriebssystemen wie XP, Vista, Server 2003 und Server 2008 - werden fast alle Stop-Fehler von fehlerhaften Treibern oder von sehr systemnaher fehlerhafter Software verursacht, oder - was noch schlimmer ist - von tatsächlich physisch schadhaften Hardwarekomponenten.

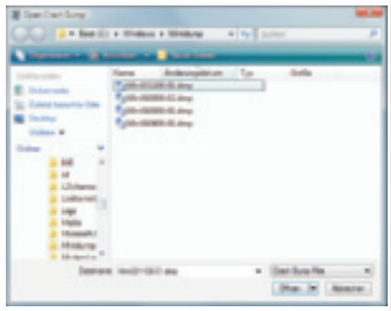
Egal, was schuld ist, für mich als Trainer und Vortragender sind Bluescreens vor allem lästig und mitunter peinlich. In anderen Situationen - zum Beispiel wenn durch einen Bluescreen Daten verloren gehen - kann so ein Stop Fehler sogar massiven Schaden anrichten.

Doch wie wird man aus den Crash Dump-Daten schlau? Woher weiß man, welcher Treiber daran schuld ist?

Nicht immer gibt der *Blue Screen of Death* selbst diese Auskunft.

Oft ist das einfacher, als man ob der kryptischen Daten vielleicht meint. Dieser Guide soll eine Anleitung dazu geben.

1. Zunächst besorgen wir uns die Debugging Tools für unsere Plattform:
   http://www.microsoft.com/whdc/devtools/debugging/installx86.mspx (32Bit)
   http://www.microsoft.com/whdc/devtools/debugging/install64bit.mspx (64Bit)
2. Dann starten wir **windbg** - Wichtig: Als Administrator ausführen!
3. Im ***File Menü***, klicken wir auf ***Symbol File Path***.
4. Im ***Symbol Path***-Fenster geben wir folgendes ein:
   "srv*c:\cache*http://msdl.microsoft.com/download/symbols;"
   und bestätigen mit *'ok'*.
5. Im ***File Menü*** wählen wir ***"open crash dump..."*** und wählen unter **c:\Windows\Minidump** das File aus, das wir analysieren wollen - in der Regel das Neueste.

   Bei mir gab es ja schon einige Crashes - es wird also Zeit, dass ich dem Übeltäter auf die Spur komme. Für jeden Crash liegt ein Crash Dump File mit einem Namen wie **Mini102107-03.dmp** in dem Verzeichnis.
6. Jetzt ein paar Sekunden auf das Ergebnis warten - Falls die Firewall sich meldet - es wird versucht auf die Symbol Files unter **msdl.microsoft.com/download/symbols** zuzugreifen - muss man die Firewall Warnung bestätigen, **windbg** schliessen und noch einmal bei Punkt 2 weiter machen.
7. Im Ergebnisfenster sucht man die Zeile ***"Probably caused by: "*** - Danach steht der Übeltäter fest.

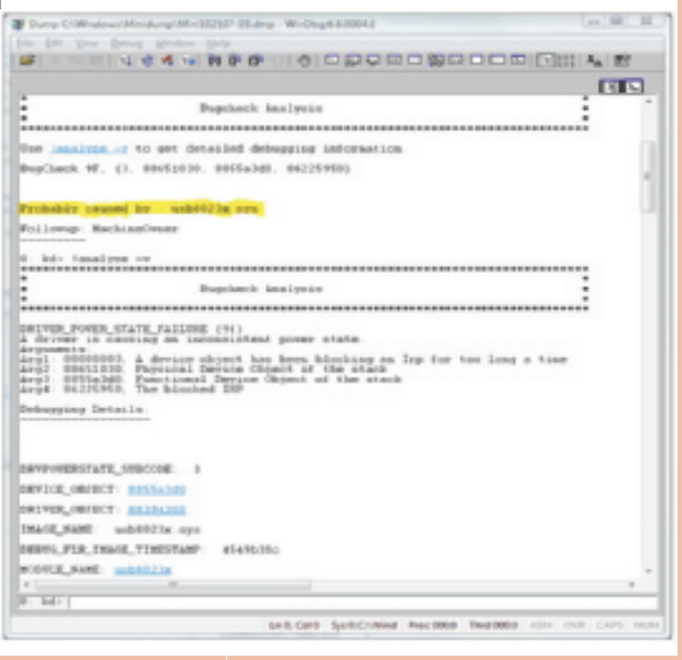
Mit einer guten Suchmaschine findet man schnell Näheres heraus, dann einfach eine neue Treiberversion vom Hersteller herunter laden und das Problem sollte behoben sein.

Möchte man mehr wissen, kann man noch **„!analyze –v"** ausführen und bekommt dann noch genauere Hinweise:

In diesem Fall war also bei mir der Übeltäter **usb8023x.sys** - der Remote NDIS USB driver. In einem anderen Fall **dne2000.sys** - ein Teil einer Sonicwall VPN Client Software.

Eine neuere Version des Treibers/der Software vom Hersteller herunter laden oder die betroffene Software deinstallieren und das Problem ist meistens gelöst.

Sollte man unter ***„probably caused by"*** die Phrase ***„memory corruption"*** finden, sollte man den Speicher, die Festplatte, die Thermik und das Bios (ungefähr in der Reihenfolge) überprüfen.



10 Systemdateien

Windows Resource Protection (WRP) versucht, wichtige Windows-Dateien, Ordner und Registry-Schlüssel vor Manipulation zu schützen. WRP ist in Windows Vista und Windows Server 2008 der Nachfolger von *Windows File Protection* (WFP), welches es schon seit Windows 2000 gibt.

Wenn eine mit WRP geschützte Datei korrupt oder fehlerhaft ist, kann es beim automatischen WRP-Reparaturvorgang zu Problemen kommen, und das kann dazu führen, dass Windows Vista nicht richtig funktioniert oder nicht mehr richtig reagiert.

Hier eine Kurzfassung der unter `http://support.microsoft.com/kb/929833/de` bzw. `http://support.microsoft.com/kb/929833/en-us` beschriebenen Lösung:

`sfc /scannow`
Überprüft Windows Systemdateien und ersetzt falsche/korrupte Dateien durch Richtige

`findstr /C:"[SR] Cannot repair member file" %windir%\logs\cbs\cbs.log >sfcdetails.txt`
Durchsucht das Protokoll, ob beim letzten Schritt irgendwelche Systemdateien nicht repariert werden können

`edit sfcdetails.txt`
Zeigt die Ergebnisse an - wenn nichts drinnen steht, ist alles in Ordnung, wenn man darin einen Dateinamen findet,
z.B. **`C:\windows\system32\jscript.dll`**

`takeown /f Path_And_File_Name`
also konkret zum Beispiel

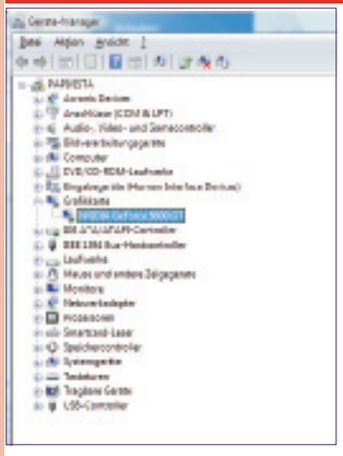
`takeown /f E:\windows\system32\jscript.dll`

Ownership übernehmen

`icacls Path_And_File_Name /GRANT ADMINISTRATORS:F`
Dateirechte für den Administrator setzen.

`Copy Path_And_File_Name_Of_Source_File Path_And_File_Name_Of_Destination`
Datei durch eine gute Version, z.B. von einer anderen Vista-Installation oder von der Windows-DVD ersetzen.

11 Treiber



Es kann manchmal sein, dass neuere Treiber ein Problem beheben - daher sollte man sich mit Hilfe von Windows Update oder auf der Homepage des Herstellers nach neueren Treibern umsehen. Aber Achtung: Manchmal ist genau das Umgekehrte der Fall - bei meinem Media Center kommt es mit dem neuesten Grafikkartentreiber zu Problemen, weshalb ich auf den letzten (älteren) Treiber zurückgerollt habe.

Das macht man übrigens im ***Geräte-Manager***.

12 Bios

Wenn man sich die Revisionshistorie von Bios Versionen so durchliest, entdeckt man, dass Probleme oft durch Fehler im Bios entstehen, und durch neuere Bios-Versionen behoben werden. Vor allem so ein Text im **`Readme.txt`** eines Bios-Updates sollte zu denken geben:

`"Solved problems: Fixed problem that the system hangs up occasionally when it is shutting down by using SIID $1:OFFx."`
Das heißt, ein Bios Update ist in jedem Fall eine gute Idee, außerdem sollte man das Bios auf Werkseinstellungen zurücksetzen, um sicherzustellen, dass nicht eine "falsche" Bioskonfiguration den Fehler verursacht.

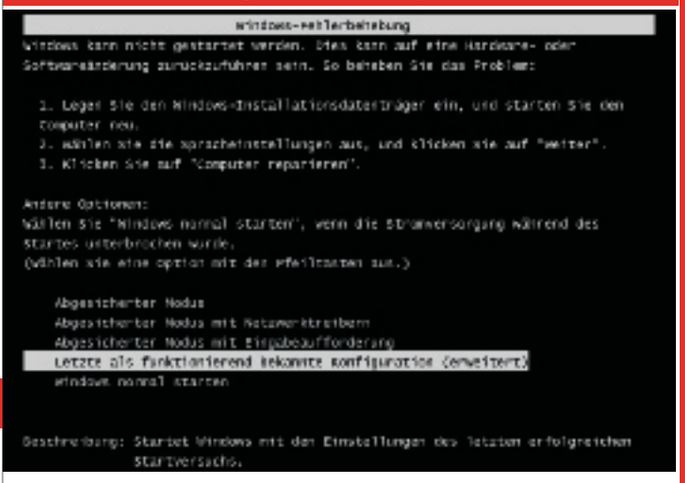
13 Microsoft Knowledgebase konsultieren

Gut, hätte man vermutlich auch schon in Schritt 1 gefunden, aber bei komplexeren Problemen kann es mitunter helfen, diese direkt in der Microsoft Knowledgebase unter `http://support.microsoft.com` nachzuschlagen.

Wichtig: Oft sind die Einträge der Knowledgebase maschinell übersetzt, und dann findet man mit einer deutschen Fehlermeldung nichts. Ich versuche daher, zunächst mit Hilfe von Google die englische Version meiner Fehlermeldung zu finden und suche dann nach der in der Knowledgebase. Oder ich verkürze die Fehlermeldung auf ein paar eindeutige Stichwörter, die auch in der englischen Version enthalten sein müssten.

Bei jedem Knowledgebase-Artikel kann man am Ende statt **„/de"** **„/en-us"** an den Link anhängen und bekommt dann den Originaleintrag. Die maschinell Übersetzten sind fast immer unbrauchbar.

14 Windows Fehlerbehung / Erweiterte Startoptionen



Spezialfälle, wo viele der Schritte nicht anwendbar sind, können zum Beispiel sein, dass das System nicht mehr startet, oder dass Bluescreens so rasch auftreten, dass man keine Zeit zur Fehleranalyse und -behebung hat.

Dann muss man zu härteren Mitteln greifen und davon gibt es auch einige:

- **Letzte funktionierende Konfiguration**

Diese Option stellt Registrierungsinformationen und Treibereinstellungen wieder her, die beim letzten erfolgreichen Start des Computers vorhanden waren. Dazu werden alle Schlüssel unterhalb von **`HKEY_LOCAL_MACHINE\System\CurrentControlSet`** durch eine ältere Version ersetzt.

- **Abgesicherter Modus**

Wenn gar nichts anderes mehr dazu führt, dass Windows hochfährt, kann man den abgesicherten Modus verwenden. Der abgesicherte Modus ist eine Methode, bei der Windows nur mithilfe von Basisdateien und -treibern gestartet wird.

Von dort aus kann man dann weitere Schritte zur Fehlerbehebung setzen, z.B. **`rstrui.exe`** ausführen, um die Systemwiederherstellung zu starten. (Mehr zur Systemwiederherstellung im nächsten Schritt.)

Sowohl zu der Option ***„Letzte als funktionierend bekannte Konfiguration"*** als auch zu der Option ***„Abgesicherter Modus"*** gelangt man automatisch, wenn das System nicht vollständig hochgefahren, oder während des Betriebs abgeschaltet (also nicht ordentlich heruntergefahren) wird.

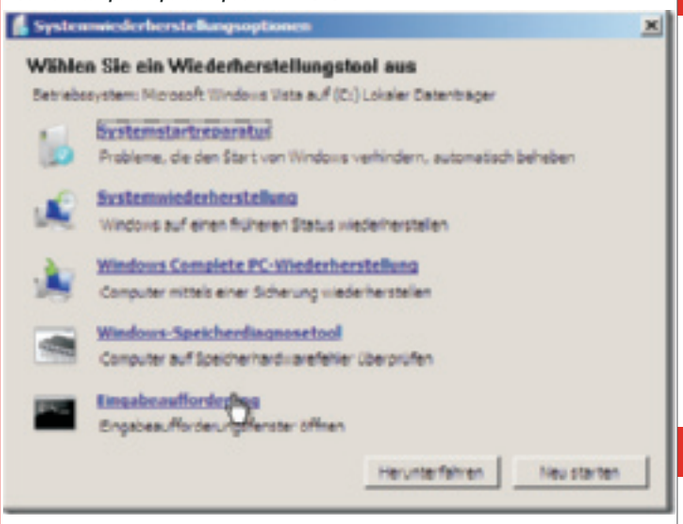
Sonst muss man nur beim Hochfahren, möglichst rasch – noch bevor das Windows Logo bzw. der Fortschrittsbalken kommt – F8 drücken, um zu den ***„Erweiterten Startoptionen"*** zu gelangen.

15 Wiederherstellung

Nur Windows Vista

Noch mehr Möglichkeiten als bei den erweiterten Startoptionen beim Systemstart bieten die Systemwiederherstellungsoptionen auf der Vista DVD. Um dort hinzukommen, muss man folgende Schritte durchführen:

1. Von Vista DVD booten
2. Sprachauswahl tätigen und auf *"Weiter"* klicken
3. Auf *"Computerreparaturoptionen"* klicken



Systemstartreparatur

Der erste Punkt, die ***Systemstartreparatur*** versucht automatisch, das System so zu reparieren, dass es wieder starten, also erfolgreich vollständig hochfahren kann.

Systemwiederherstellung

Diese Option geht viel weiter als ***„Letzte funktionierende Konfiguration"***, weil sie nicht nur einen Teil der Registry, sondern Windows-Systemdateien, Programme und Registrierungseinstellungen komplett wiederherstellt. Dabei muss dieses Feature aber aktiviert sein, und es müssen auch Wiederherstellungspunkte vorhanden sein. Diese Wiederherstellungspunkte können manuell oder regelmäßig erstellt werden, werden aber auch automatisch zum Beispiel bei einer Software- oder Treiberinstallation angelegt. Wie viele Wiederherstellungspunkte zur Verfügung stehen, hängt auch vom verfügbaren Platz auf der Festplatte ab.

Benutzerdaten sind von der Systemwiederherstellung nicht betroffen.

Windows Complete PC-Wiederherstellung

Vermutet man den Fehler auf Softwareseite und reichen Maßnahmen wie ***„Letzte funktionierende Konfiguration"*** oder Systemwiederherstellung nicht aus, um ein Problem zu beseitigen, kann man auch das komplette Festplatten-Image mit Hilfe der Backup Funktion ***„Windows Complete PC-Wiederherstellung"*** wiederherstellen.

Vorsicht: Hierbei sind auch Benutzerdateien betroffen, so dass es wichtig ist, dass man zusätzlich noch über Backups der Benutzerdateien verfügt. Dafür gibt es in Vista das Feature der ***automatischen Dateisicherung***.

Ich verwende die *Windows Complete* PC-Sicherung übrigens immer, wenn ich ein System neu aufsetze, um das komplett installierte und konfigurierte System als Komplettimage zu sichern.

Windows Speicherdiagnosetool

Das Speicherdiagnosetool wurde schon unter ***Punkt 5: Hauptspeicher/Memory*** besprochen, lässt sich aber natürlich auch von hier aus starten

Eingabeaufforderung

Es gibt dann noch einige Dinge für die man eine Kommandozeile braucht. – `copy/xcopy/robocopy` zum Beispiel für das Kopieren/Spiegeln/Wiederherstellen von Dateien. Oder `regedit`, falls man einmal bei der Registry Hand anlegen muss, um zum Beispiel den Massenspeichertreiber (SATA/Raid) zu verstellen.

Zum Beispiel kann man Probleme mit SATA-Treibern - wie dem Stop Fehler `0x0000007B` - zu Leibe rücken, indem man im Bios auf AHCI umstellt und dann in der Registry unter `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Msahci` den Value von *'Start'* auf *'0'* setzt.

Fazit: Dank der Systemwiederherstellungsoptionen kann eine Vista-DVD fast als *„Schweizer Taschenmesser"* im Troubleshooting bezeichnet werden. Nur Microsoft's DART *(Diagnostic and Recovery Toolset)* – ehemals ERD Commander kann noch mehr, ist aber nur für Microsoft's Unternehmenskunden mit *Software Assurance* Vertrag gegen Bezahlung erhältlich.

16 Neu installieren

Zu Testzwecken das Betriebssystem neu installieren, am besten mit einer zweiten Festplatte.

Möglichst nur in Windows Vista enthaltene bzw. über Windows Update angebotene, WHQL-zertifizierte Treiber einsetzen, Systemstabilität beobachten.

Wenn das System tagelang stabil bleibt, nach und nach Software und fehlende Treiber installieren beziehungsweise durch neuere Treiber vom Hardwarehersteller aktualisieren - Wenn man da nicht zu viel auf einmal macht, kann man mit Hilfe von ***Schritt 3 (Zuverlässigkeitsüberwachung)*** vielleicht einen zeitlichen Zusammenhang zwischen der Installation eines Treibers oder eines Programms und den Abstürzen erkennen.

Um diesen Schritt zu beschleunigen, verwende ich übrigens einen schnellen USB Stick und eine `autounattend.xml` Datei, die das Setup vollständig automatisiert. So ist in nur 5-7 Minuten Windows Vista installiert.

17 Hersteller/Service

Wenn nach einer Neuinstallation die Probleme gleich wieder auftauchen, ist von einem Hardwaredefekt auszugehen, man sollte dann das Gerät einmal vom Hersteller unter die Lupe nehmen lassen, vielleicht überhitzt es sich regelmäßig oder es ist das Mainboard oder ein elektronischer Bauteil defekt?

18 Microsoft Support

In ganz seltenen Fällen könnte man tatsächlich von einem Bug des Betriebssystems betroffen sein, der so selten auftritt, dass man ihn nur mit Hilfe eines speziellen Patches beheben kann, den man aber nur vom telefonischen Microsoft Support auf Anforderung zugeschickt bekommt, wenn dieser meint, dass der Patch das Problem lösen könnte.

Wenn man ohnehin einen Supportvertrag mit Microsoft oder kostenlose Supportanfragen hat, kann dieser Schritt natürlich auch viel früher erfolgen. Trifft die Schuld wirklich Microsoft, bekommt man die Anfrage wieder gutgeschrieben. Hat man keine Support-Calls, muss man aber löhnen, und geht das Risiko ein, dass man das nicht wieder gutgeschrieben bekommt, wenn es eben doch kein Bug im Betriebssystem ist.

Auch wenn da jetzt ein ganz schön ausführliches Nachschlagewerk entstanden ist - Bei manchen Themen konnte ich nur an der Oberfläche kratzen, und empfehle daher mein Blog (`http://blog.this.at/`) für weitergehende Informationen.

Für Fragen und Anregungen stehe ich im Forum (`http://www.clubcomputer.at/`) von ClubComputer gerne zur Verfügung.

Messtechnik für den Profi:

- Netzqualitätsanalyzer
- Transientenrekorder
- Energieanalyzer
- Schutzmaßnahmen-prüfgeräte
- Schreiber
- Einbauanalyzer
- Stromzangen

Mobile Computer für alle Fälle:

- Notebooks
- Industrie-Notebooks
- Sonderlösungen

MTM SYSTEME

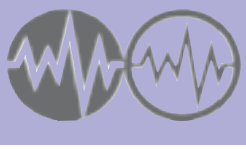
Mikrocontroller, Entwicklungstools und Baugruppen:

- Compiler
- Debugger
- Betriebssysteme
- Starterkits
- Minimodule

Familien:
C166 & ST10
8051, C500, C800
M16C, 77k,TLCS900
TriCore, Carmel
MIPS, DSP56xxx,
68xxx, PowerPC

Wir entlasten Sie mit folgenden Dienstleistungen:

- Messen und Protokollieren der Netzqualität
- Auffinden von Netzstörungen
- Schulungen zum Thema Netzqualität
- Produktschulungen



MTM-Systeme
Ing. Gerhard Muttenthaler
Hadrawagasse 36
1220 Wien

fon +43 1 2032814
fax +43 1 2021303
mail office@mtm.at
web www.mtm.at

Produktinformationen und Nützliches unter:
www.mtm.at

NEUE INFINEON STARTERKITFAMILIE

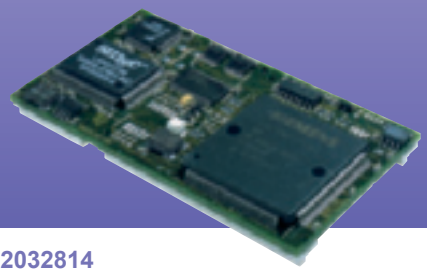
Zur neuen XC16xFamilie sind nun auch die Starterkit's erhältlich.

Die Starterkits für XC161CI, XC164CS und XC167CI werden "ready to use" incl. Software geliefert

Der optimale Start für Ihre 16 Bit Mikrocontrolleranwendung!

16-Bit Applikationen mit Ethernet-Anbindung

Mit dem TQM167UE bietet TQ-Components ein voll lauffähiges embedded 16-Bit Microcontroller System mit Ethernet-Schnittstelle auf einer Fläche von nur 80 x 44 mm² an. Als Systemkern dient der Infineon SAB-C167CR Microcontroller. Der Speicherausbau von 1 MB SRAM sowie 1 MB FLASH erlaubt auch größere Programme laufen zu lassen. Die RS232 Schnittstelle und 4-fach UART stellen die komplette Verbindung zur Außenwelt des Moduls her. Das TQM167UE bietet zusätzlich den Super I/O-Contoller FDC37C669, z.B. zur Anbindung eines Floppy-Laufwerks.
Besonders einfach ist das Programmhandling. Über die mitgelieferte Download-SW können eigene Programme einfach und komfortabel auf das Modul geladen werden. Um den Einstieg in die Modulwelt zu vereinfachen, liefert TQ-Components das Starterkit zu oben beschriebenem Modul, die komplette "Plug and Play" Lösung unter der Bezeichnung STK167UE.



Info bei MTM-Systeme unter www.mtm.at oder +43 1 2032814

Die perfekte Schutzsoftware
für Windows-PCs - umfassend und dennoch variabel!

NOCH KOMFORTABLER!

**Mit neuen Betriebsmodi,
USB-Kontrolle,
Admin-ServiceKey und
dem HDGUARD.master
mit Lehrerkonsole**

HDGUARD.master mit Lehrerkonsole und didaktischen Funktionen

- USB-Kontrolle
- Bildschirme dunkel/ hell schalten
- Internet sperren/ freischalten

HDGUARD und HDGUARD.master
Für einzelne Windows-PC und ganze Unterrichtsnetzwerke

Nach jedem Neustart stehen die PCs in einem sauberen Originalzustand wieder zur Verfügung.

- Hochwirksamer PC-Schutz gegen Datenverluste durch Viren oder schädigende Manipulationen
- Signifikante Reduktion von Administrationsaufwand und -kosten
- Arbeitet voll automatisch und restauriert den PC bei jedem Neustart
- Ständige Verfügbarkeit der PCs - ohne zusätzliche Hardware - ohne Desktopbeschränkungen
- Manuelle Zusatzmodi für Softwaretests oder Seminarbetrieb
- Komfortabel bei der PC-Wartung durch USB-ServiceKey, USB-Kontrolle und die zentrale Steuerung mit HDGUARD.master

30 Tage KOSTENFREI testen!

STADLER EDV

STADLER EDV-Dienstleistungs- und Handelsges.m.b.H.
Welschgasse 3/1/7, A-1230 Wien
Tel: +43 (0) 1 865 3990-0, Fax: +43 (0) 1 865 3990-123
Kontakt: office@systemsoftware.at Internet: www.systemsoftware.at