

Manual PDF (translation in progress,  
come back soon)

without tutorial

# 1: Install-Backup

## 1.1 Tutorial (online)

1. [Backing up Windows®](#)
2. [Install-Restore DVD](#)

## 1.2 Frequently Asked Questions (Online)

- ▢ [Install-Backup FAQ](#)

## 1.3 Command Line

```
rtcmd ib [-CONTROL] [p=PASSWORD] t[TCONTROL]=TARGET ...
```

Install-Backup archiviert die Software eines Rechners. Dazu gehört das gesamte Windows® Betriebssystem und die installierten Programme.

```
rtcmd ib
```

Die Installation wird im aktuellen Verzeichnis archiviert.

### 1.3.1 CONTROL

Allgemeine Optionen, Kombination aus folgenden Buchstaben:

Archivierung	
<b>b Binary Check</b>	Alle Dateien werden Bit für Bit geprüft.
<b>f Forensic Check</b>	Like Binary Check, a message box appears before files are replaced.
<b>n New</b>	Benutzt keine <a href="#">Templates</a> .
<b>p Password</b>	Aktiviert die <a href="#">Zip-Verschlüsselung</a> und bittet um die Eingabe Ihres <a href="#">Passwortes</a> .
<b>x eXtended</b>	The content of Reparse Points and Volume Mount Points will be added to the backup.
Dialog	
<b>i[x] Integrate</b>	Kein Benutzerdialog. Die <a href="#">Integrationszahl x</a> bestimmt, ob Fehlerfenster, Warnfenster oder der Assistent angezeigt werden.
<b>o[x] Optional</b>	Die Vorgaben der Command Line können im Assistent verändert werden. Unter der Optionszahl x merkt sich der Assistent die veränderten Einstellungen.
Protokoll	
<b>q Quiet</b>	Zeigt nur eine Start- und Stopp-Meldung an. Schreibt bei Erfolg ein Protokoll nach <a href="#">RT_LOG</a> und im Falle eines Fehlers nach <a href="#">RT_ERROR</a> .
<b>t Talk</b>	Zeigt <a href="#">Berechtigungen</a> an.

```
rtcmd ib -pi3
```

Install-Backup fragt nach dem Passwort für die Zip-Verschlüsselung(p). Das Programm wird ohne den Assistenten gestartet, bei Fehlern und Warnungen erscheint ein entsprechendes Fenster(i3).

### 1.3.2 PASSWORD

Aktiviert die Zip-Verschlüsselung und übergibt ein Passwort.

```
rtcmd ib p=38zec47xc662
```

Die laufende Installation wird zip-verschlüsselt im aktuellen Verzeichnis gesichert.

### 1.3.3 TCONTROL

Zieloptionen, siehe [TCONTROL](#) bei [Private-Backup](#).

### 1.3.4 TARGET

Zielordner. Ein Zielordner muss immer mit '.ib' enden um eindeutig als Installationssicherung identifiziert zu werden.

```
rtcmd ib t=Windows.ib
```

Die Installation wird im Ordner Windows.ib gesichert.

Wie bei Private-Backup können [mehrere Ziele](#) angegeben und [Joker](#) eingesetzt werden.

Command Line für Install-Backup im Kontextmenü von Arbeitsplatz bzw. Computer:

```
rtcmd ib -o1 tf5=*HD\*ARCH\ tof5=*NET\*ARCH\ to=*RD\*ARCH\ to=*CD\*ARCH\
```

## 2: Install-Restore

### 2.1 Tutorial (online)

1. [Restoring Windows®](#)
2. [Additional Windows® Environment](#)
3. [Moving Windows® to new Hardware](#)

### 2.2 Frequently Asked Questions (Online)

- [Install-Restore FAQ](#)

### 2.3 Command Line

```
rtcmd ir [-CONTROL] [t=TARGET] [s=SOURCE] ...
```

Install-Restore stellt eine Installation von einem Install-Backup Datensatz wieder her. Der Install-Backup Datensatz muss sich in einem Ordner mit der Endung '.ib' befinden.

```
rtcmd ir
```

Stellt die Installation vom aktuellen Ordner her. Öffnen Sie eine Console mit einem Rechts-Klick auf einen .ib Ordner, um dieses Kommando zu verwenden.

Install-Restore verfügt über zwei Methoden, von denen die richtige normalerweise automatisch ausgewählt wird:

- **Install-Soft-Restore** geht davon aus, dass sich die Hardware nicht verändert hat. Diese Methode ist richtig, wenn Install-Restore auf demselben Rechner ausgeführt wird, von dem der Datensatz stammt.
- **Install-Hard-Restore** adaptiert die Hardware Einstellungen wie z.B. Treiber für den Mikroprozessor oder die Bildschirnkarte an die neue Installation. Diese Methode ist richtig, wenn Install-Restore auf einem anderen Rechner ausgeführt wird.

Anhand der Seriennummer der Festplatte wird erkannt, ob die Wiederherstellung auf fremder Hardware durchgeführt wird. Dann wird automatisch auf Hard Restore umgeschaltet. Hard Restore kann nur mit derselben Windows® Version und demselben Servicepack ausgeführt werden.

Install-Restore setzt die wiederhergestellte Installation als Vorauswahl in das Bootmenü. Dadurch wird die neue Installation beim nächsten Start des Rechners automatisch gewählt, sofern Sie während des Startvorgangs keine andere Auswahl treffen.

Wird als Ziel eine andere Festplatte, als die auf der sich das aktuelle Startlaufwerk befindet angegeben, so werden alle Startdateien auf der Zielfestplatte aktualisiert. Das System kann dann nach einem Ausfall der aktuellen Festplatte auch von der Zielfestplatte gestartet werden.

#### 2.3.1 CONTROL

Optionen, Kombination aus folgenden Buchstaben:

Wiederherstellung	
<b>b Binary Check</b>	Alle Dateien werden Bit für Bit geprüft.
<b>d Default</b>	Setzt die neue Installation als Vorauswahl in das Bootmenü.
<b>f Forensic Check</b>	Like Binary Check, a message box appears before files are replaced.
<b>h Hard</b>	aktiviert die Treiber-Anpassung (Hard-Restore).
<b>n New</b>	Ersetzt alle Dateien, auch solche, die sich nicht verändert haben.
<b>x eXtended</b>	Restore includes the content of Reparse Points and Volume Mount Points.
Dialog	
<b>i[x] Integrate</b>	Kein Benutzerdialog. Die <a href="#">Integrationszahl x</a> bestimmt, ob Fehlerfenster, Warnfenster oder der Assistent angezeigt werden.
<b>o[x] Optional</b>	Die Vorgaben der Command Line können im Assistent verändert werden. Unter der Optionszahl x merkt sich der Assistent die veränderten Einstellungen.
Protokoll	
<b>q Quiet</b>	Zeigt nur eine Start- und Stopp-Meldung an. Schreibt bei Erfolg ein Protokoll nach <a href="#">RT_LOG</a> und im Falle eines Fehlers nach <a href="#">RT_ERROR</a> .

<b>s Stop</b>	Auto Reboot nach Blue Screen wird deaktiviert.
<b>t Talk</b>	Zeigt <a href="#">Berechtigungen</a> an.

```
rtcnd ir -hd
```

Install-Restore startet im Hard-Restore Modus. Die neue Installation wird in das Bootmenü eingetragen, und als Vorauswahl gesetzt.

### 2.3.2 SOURCE

Pfad, in dem sich der Datensatz befindet, der wiederhergestellt werden soll.

```
rtcnd ir s=C:\RtArch\_PC\Vista_32\091026_072130.ib
```

Der Pfad darf [Archiv-](#) und [Objektjoker](#) enthalten.

```
rtcnd ir s=C:\*ARCH\*
```

Verwendet den neusten Datensatz des aktuellen Betriebssystems für die Wiederherstellung.

### 2.3.3 TARGET

Zielordner, in denen die Installation wiederhergestellt werden soll.

<b>t=*</b>	Die Installation wird in den selber Ordnern wiederhergestellt, von denen die Sicherungskopie stammt. Verwenden Sie diese Zieleinstellung für die Wiederherstellung von Domainservern mit Active Directory, da dieses in den selben Ordnern wiederhergestellt werden sollte, von denen es stammt. Kopieren Sie eine Installation vor dem Aufsetzen des Active Directory in andere Ordner (z.B. t=C:\dom...) um mehrere Domainserver oder Windows® Systeme auf einer Festplatte zu nutzen.
<b>t=D:\</b>	Die Installation wird auf Laufwerk D:\ wiederhergestellt. Es werden die original Ordernamen verwendet.
<b>t=C:\vis...</b>	Die Installation wird auf Laufwerk C:\ wiederhergestellt. Die neuen Systemordner beginnen mit 'vis' und werden automatisch sinnvoll verlängert.

Ohne TARGET wird die Installation in den original Ordner (z.B. c:\Windows,..) wiederhergestellt.

## 3: Private-Backup

### 3.1 Tutorial (online)

1. [Selecting backup media](#)
2. [Backup](#)
3. [The Log](#)
4. [Encrypting File System](#)
5. [Zip Encryption](#)

### 3.2 Frequently Asked Questions (Online)

- ▮ [Private-Backup FAQ](#)

### 3.3 Command Line

```
rtcmd pb [-CONTROL] [p=PASSWORD] s=SOURCE [t[TCONTROL]=TARGET] ...
```

Private-Backup stores a folder or a drive in one or multiple [Zip files](#). EFS encrypted data is guaranteed to be stored encrypted.

```
rtcmd pb s=Mails
```

The folder Mails will be stored in a [Zip file](#).

#### 3.3.1 CONTROL

General Options, a combination of the following characters:

Backup	
<b>a Access Control</b>	<a href="#">Access Control Lists</a> are backed up.
<b>b Binary Check</b>	All files are scanned bit by bit
<b>f Forensic Check</b>	Like Binary Check, a message box appears before files are replaced.
<b>m Move</b>	Deletes the original folder after successful backup.
<b>n New</b>	No <a href="#">Template</a> .
<b>u Update</b>	Private-Backup will be aborted with OK if nothing has changed compared to the <a href="#">Template</a> .
<b>tx Targets</b>	At least x targets must exist.
<b>v VSS</b>	<a href="#">VSS</a> is activated immediately. Without this option, VSS is activated only when a source file is being opened.
<b>x eXtended</b>	The content of Reparse Points and Volume Mount Points will be added to the backup.
Encryption	
<b>e Encrypt</b>	<a href="#">Zip files</a> on local hard drives (NTFS) will be encrypted using <a href="#">EFS</a> . All other Zip files will also be <a href="#">sealed</a> .
<b>k Key</b>	Reports an error when a file is EFS encrypted. This option is useful to backup the EFS key itself.
<b>p Password</b>	Enables <a href="#">Zip encryption</a> and asks for a password.
<b>r Raw</b>	EFS encrypted files will be backed up as <a href="#">RAW files</a> . This is the default for unencrypted folders. If you do not own the EFS key for a file, it will always be backed up as RAW file.
<b>s Seal</b>	<a href="#">Seals</a> all Zip archives with EFS. This is the default for encrypted folders.
Wizard	
<b>i[x] Integrate</b>	No user interaction. The <a href="#">integration number</a> x determines whether error messages, warnings, or the wizard will be displayed.
<b>o[x] Optional</b>	The parameters entered by the command line can be changed in the wizard. The wizard will remember these changes under the option number x.
Log File	

<b>q Quiet</b>	Displays only a start and stop message. If successful, a complete log file will be written to <a href="#">RT_LOG</a> and in case of failure to <a href="#">RT_ERROR</a> .
<b>t Talk</b>	Shows <a href="#">Access Control Lists</a> (only together with 'a').

Command line for 'Zip rt' which can be an entry in context menu for folders:

```
rtcmd pb -o3nm s=Mails
```

The folder Mails will be stored in a [Zip file](#). No template will be used. The original folder will be deleted after successfully backing it up. Setting in the wizard can be changed. Changes will be stored under the number 3 and reused when the wizard will be called the next time.

### 3.3.2 PASSWORD

Enables Zip encryption and passes a password.

```
rtcmd pb p=38zec47xc662 s=Mails
```

The folder Mails will be stored in a [Zip file](#) with Zip encryption enabled.

### 3.3.3 SOURCE

Folder to be saved. A source folder must always be specified. You can use [wildcards](#) here:

```
rtcmd pb "s=*DOC\Mails to Daddy"
```

```
rtcmd pb "s=C:\Users\ben\Documents\Mails to Daddy"
```

The folder "Mails to Daddy" will be saved. This folder is located in 'My Documents' (XP) or in 'documents' (beginning with Vista™). If the name of a folder contains spaces, it must be set in quotes.

### 3.3.4 TCONTROL

Target options, combination of the following characters:

<b>dX Day</b>	Delete all <a href="#">digit archives</a> in the destination folder that are older than X days.
<b>f Files</b>	Delete as many old <a href="#">number archives</a> in the destination folder, until the space for the new archive is sufficient.
<b>fX Files</b>	Keep the latest X <a href="#">digit archives</a> in the destination folder.
<b>m Memory</b>	Delete as many old archives in the destination folder, until the space for the new archive is sufficient.
<b>mX Memory</b>	Delete as many old archives in the destination folder, until the disk space required by the target folder will be less than X MB.
<b>nX Number</b>	A maximum of X targets will be selected randomly. Use this option to evenly spread the archives on the network.
<b>o[X] Optional</b>	At least X targets must be available. Without X, the complete target is optional (X = 0).

```
rtcmd pb s=Photos tm=a:\Photos\Christmas_2012.zip
```

The folder Photos will be backed up on drive F: (e.g. a USB flash drive). The name of the archive is Christmas\_2012.zip. If there is insufficient space on the drive, old zip files in the folder F:\photos will be deleted until the space is sufficient.

```
rtcmd pb s=Drawings to2n3f30=*NET\*ARCH\*
```

[Network cluster backup](#). At least 2 computers in the network must be available. If more than 3 computers are available, Private-Backup will select 3 randomly. If a destination folder contains more than 30 archives, the oldest will be deleted.

If this command runs on the user account and not on the account of a backup administrator, backup storage space for [EFS](#) encrypted data will be reduced by about 50%. This is due to the fact that encrypted data can never be compressed but a backup administrator should only be able to read encrypted data. Private-Backup tries to compress before it writes to an encrypted archive.

### 3.3.5 TARGET

Target archive, if no file name is specified, the archive will be named after the folder to be backed up:

```
rtcmt pb s=Mails t=g:\
```

```
rtcmt pb s=Mails t=g:\Mails.zip
```

If a previous filename has been specified, it will be used for the following targets:

```
rtcmt pb s=Mails t=c:\January.zip t=d:\
```

```
rtcmt pb s=Mails t=c:\January.zip t=d:\January.zip
```

By specifying a file extension, the encryption for the specific target to be controlled.

```
rtcmt pb s=Mails t=G:\January.seal
```

The folder Mails will be backed up in the [sealed](#) file g:\January.seal.

An [object wildcard](#)(\*) will create a [numerical archive](#) which name consisting of the current date and time:

```
rtcmt pb s=Mails t=*
```

```
rtcmt pb s=Mails t=121025_194843.zip
```

A target path can contain [drive-](#) and [archive wildcards](#):

```
rtcmt pb s=Mails t=*HD\*ARCH
```

```
rtcmt pb s=Mails t=C:\RtArch\ben\Documents\Mails\Mails.zip  
t=D:\RtArch\ben\Documents\Mails\Mails.zip
```

The folder Mails will be backed up on all hard drives available.

Command line for Private-Backup in the context menu of folders:

```
rtcmt pb -ol s=Mails tf30=*HD\*ARCH\* tof30=*NET\*ARCH\* tof5=*RD\*ARCH\  
to=*CD\*ARCH\* tof30=*DOC\cloud\*ARCH\*
```

You can adapt the configuration of the context menu to your personal requirements by editing the [registry](#) value:

```
SOFTWARE\Reushtools\RClick\Directory\Private-Backup
```



## 4: Private-Restore

### 4.1 Tutorial (online)

1. [Restoring a folder](#)
2. [Import into new folder](#)

### 4.2 Frequently Asked Questions (Online)

- ▢ [Private-Restore FAQ](#)

### 4.3 Command Line

```
rtcmd pr [-CONTROL] [p=PASSWORD] [t=TARGET] s=SOURCE ...
```

Private-Restore stellt einen Ordner von einer [Zip-Datei](#) oder [Sealdatei](#) wieder her.

```
rtcmd pr s=Briefe.zip
```

Der Ordner Briefe wird von der [Zip-Datei](#) Briefe.zip wiederhergestellt.

#### 4.3.1 CONTROL

Steuert die Wiederherstellung des Ordners. CONTROL ist eine Kombination aus folgenden Buchstaben:

Wiederherstellung	
<b>a Access Control</b>	<a href="#">Berechtigungen</a> werden wiederhergestellt.
<b>b Binary Check</b>	Alle Dateien werden Bit für Bit geprüft.
<b>f Forensic Check</b>	Like Binary Check, a message box appears before files are replaced.
<b>m Move</b>	Löscht die <a href="#">Zip-Datei</a> nach der Wiederherstellung.
<b>n New</b>	Ersetzt alle Dateien, auch solche, die sich nicht verändert haben.
<b>x eXtended</b>	Restore includes the content of Reparse Points and Volume Mount Points.
Dialog	
<b>i[x] Integrate</b>	Kein Benutzerdialog. Die <a href="#">Integrationszahl</a> x bestimmt, ob Fehlerfenster, Warnfenster oder der Assistent angezeigt werden.
<b>o[x] Optional</b>	Die Vorgaben der Command Line können im Assistent verändert werden. Unter der Optionszahl x merkt sich der Assistent die veränderten Einstellungen.
Protokoll	
<b>q Quiet</b>	Zeigt nur eine Start- und Stopp-Meldung an. Schreibt bei Erfolg ein Protokoll nach <a href="#">RT_LOG</a> und im Falle eines Fehlers nach <a href="#">RT_ERROR</a> .
<b>t Talk</b>	Zeigt <a href="#">Berechtigungen</a> an (nur mit 'a').

Command Line für 'Unzip rt' aus dem Kontextmenü für Archive:

```
rtcmd pr -o3m s=Briefe.zip
```

Der Ordner Briefe wird von der [Zip-Datei](#) Briefe.zip wiederhergestellt. Die Zip-Datei wird nach erfolgreicher Wiederherstellung gelöscht(m). Die Einstellungen dürfen im Assistenten verändert(o) werden. Veränderte Einstellungen werden unter der Nummer 3 gespeichert.

#### 4.3.2 PASSWORD

Mit diesem Parameter kann ein [zip-verschlüsseltes](#) Archiv entschlüsselt werden. Ist das angegebene Passwort falsch, dann wird während der Wiederherstellung nach dem richtigen gefragt.

```
rtcmd pr p=38zec47xc662 s=Briefe.zip
```

### 4.3.3 SOURCE

Quellarchiv, es muss mindestens ein Archiv angegeben werden.

```
rtcmd pr s=Briefe.zip
```

Der Ordner Briefe wird von Briefe.zip wiederhergestellt.

Werden mehrere Archive angegeben, sucht Private-Restore nach dem neusten:

```
rtcmd pr s=E:\Briefe.zip s=M:\Briefe.zip
```

```
rtcmd pr s=M:\Briefe.zip
```

Endet eine Archivbezeichnung mit einem \*, dann wird in dem angegebenen Archivordner nach dem neusten Archiv gesucht:

```
rtcmd pr s=M:\Hans\Documents\Briefe\* t=*
```

```
rtcmd pr s=M:\Hans\Documents\Briefe\090810_094501.zip t=*
```

SOURCE darf [Laufwerks-](#) und [Archivjoker](#) enthalten. Diese werden mit Hilfe von TARGET aufgelöst:

```
rtcmd pr s=*RD\*ROOT\* t=Briefe
```

```
rtcmd pr s=M:\Hans\Documents\Briefe\090810_094501.zip t=Briefe
```

Command Line für 'Private-Restore' aus dem Kontextmenü für Ordner:

```
pr -ol t=Briefe s=*HD\*ARCH\* s=*NET\*ARCH\* s=*RD\*ARCH\* s=*CD\*ARCH\*
```

Sucht das neuste Archiv und stellt den Zielordner wieder her.

Um auch auf Disketten zu suchen, kann die Command Line um

```
s=*FD\*ARCH\*
```

erweitert werden.

### 4.3.4 TARGET

Zielordner, dieser Parameter ist optional. Wird kein Zielordner angegeben, dann wird der Ordner mit dem Namen der Zip-Datei im aktuellen Verzeichnis wiederhergestellt:

```
rtcmd pr s=Briefe.zip
```

```
rtcmd pr s=Briefe.zip t=Briefe
```

Mit einem \* als Ziel wird der original Ordner wiederhergestellt. Dies setzt aber voraus, dass die [Zip-Datei](#) mit Private-Backup erstellt wurde:

```
rtcmd pr s=Briefe.zip t=*
```

```
rtcmd pr s=Briefe.zip t=C:\Users\Hans\Documents\Briefe
```

## 5: Console-Editor

### 5.1 Handling

#### 5.1.1 Protokoll

Jede Console wird protokolliert. Das Protokoll beginnt mit einem Zeitstempel und dem Namen des Rechners, auf dem das Programm ausgeführt wurde und dem Namen des Benutzers.

```
091031_164920      Elefant\Hans
```

Es endet mit einem Zeitstempel und dem **Exit-Code** des Programms.

```
091031_164925      exit 0
```

Der Inhalt einer Console wird bei ERFOLG nach **RT\_LOG** und bei VERSAGEN nach **RT\_ERROR** protokolliert. Der SCHEDULE Status wird nach **RT\_SCHEDULE** protokolliert.

Sind diese Umgebungsvariablen nicht gesetzt, werden die Voreinstellungen verwendet:

	Exit	Beispiel
<b>Console sichtbar</b>	0	C:\RtArch\Hans\_LOG_\Console\091025_194843.log
	1	C:\RtArch\Hans\_ERROR_\Console\091025_194843.log
<b>Console unsichtbar</b>	0	C:\RtArch\Hans\_LOG_\Hidden\091025_194843.log
	1	C:\RtArch\Hans\_ERROR_\Hidden\091025_194843.log
<b>SCHEDULE</b>		C:\RtArch\Hans\_SCHEDULE_\eEE010B5C.log

Ein Fehler im Programm `c_e.exe` oder dessen Hilfsprogramm `RtHost.exe` wird nach **RT\_ERROR** protokolliert:

	Beispiel
<b>c_e.exe</b>	C:\RtArch\Hans\_ERROR_\c_e\071025_194843.log
<b>RtHost.exe</b>	C:\RtArch\Hans\_ERROR_\RtHost\071025_194843.log

Sollte ein Fehler aufgrund eines Softwareproblems auftreten, senden Sie bitte das Protokoll an [support@reushtools.com](mailto:support@reushtools.com).

#### 5.1.2 Windows® PowerShell™

```
c_e -x *DOC\ PowerShell
```

Erstellen Sie eine Verknüpfung oder einen **Hotkey** mit diesem Befehl, um PowerShell™ im Ordner Eigene Dateien(XP) bzw. Dokumente(Vista™) zu starten.

#### 5.1.3 Cygwin Bash Shell

Um eine Cygwin Bash Shell mit Console-Editor zu starten, genügt ein Klick auf die Cygwin Verknüpfung, die bei der Installation von Cygwin erstellt wird.

#### 5.1.4 Input-Scripts

Bei der Standardinstallation werden verschiedene Dateiendungen mit Console-Editor verknüpft. Dadurch werden beim Start eines Scripts abhängig von der Dateiendung verschiedene Parameter abgefragt und an das Script übergeben.

	%1	%2
<b>.pcmd</b>	einfaches Passwort	
<b>.ppcmd</b>	doppeltes Passwort	
<b>.ecmd</b>	offener Parameter	
<b>.epcmd</b>	offener Parameter	einfaches Passwort
<b>.eppcmd</b>	offener Parameter	doppeltes Passwort

```
@echo off
```

```
rtcmd pb "p=%1" s=Briefe
```

Dieses Script mit der Dateiendung .ppcmd fragt den Benutzer zweimal nach seinem Passwort für die Zip-Verschlüsselung.

### 5.1.5 Scripts beim Abmelden oder Herunterfahren

Console-Editor bietet die Möglichkeit ein Programm zu starten und nach erfolgreicher Ausführung das Benutzerkonto abzumelden, den Rechner auszuschalten oder herunterzufahren. Dazu kann eine [Verknüpfung im Startmenü](#) oder ein [Hotkey](#) angelegt werden:

```
c_e -hl *DOC\ rtcmd pb -i s=data tf30=*HD\*ARCH\*
```

Sichert den Ordner data und meldet den Benutzer ab.

```
c_e -ht rtcmd ir -i s=C:\*ARCH\*
```

Stellt die Installation wieder her und schaltet den Rechner aus.

Im Gegensatz zu Scripts mit [Gruppenrichtlinien](#) wird auch beim Herunterfahren des Rechners das aktuelle Benutzerkonto verwendet. Somit ist auch das Netzwerk für die Datensicherung und Protokollierung voll vorhanden.

### 5.1.6 Scripts mit Gruppenrichtlinien starten

Nicht bei XP Home.

Eine Gruppenrichtlinie bietet eine gute Möglichkeit z.B. beim Abmelden ein Private-Backup Script und beim Herunterfahren ein Install-Restore Script zu starten:

- 'mmc' öffnet Microsoft Management Console.
- Datei->Snap-In hinzufügen/entfernen
- Hinzufügen->Gruppenrichtlinienobjekt-Editor

Unter diesen Menüpunkten können Scripts verwaltet werden:

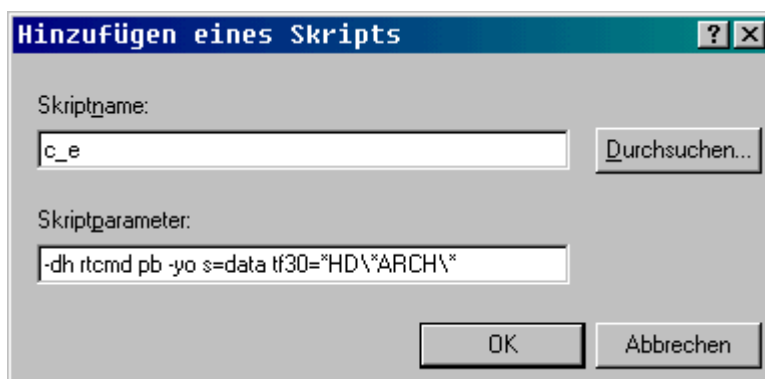
- Computerkonfiguration->Windows-Einstellungen
- Benutzerkonfiguration->Windows-Einstellungen

Die Verwendung von Console-Editor bringt zwei wichtige Vorteile:

- Im Fehlerfall wird eine Meldung an den Benutzer ausgegeben.
- Die Protokolle können über das Netzwerk verschickt werden, Fehlerprotokolle landen z.B. direkt auf dem Schreibtisch des Administrators.

Achtung! Scripts, die beim Starten oder Herunterfahren ausgeführt werden, sind anonym. Auf das Netzwerk kann deshalb nur über das Gastkonto zugegriffen werden.

Mit diesem Kommando werden die Ordner 'data' automatisch beim Abmelden archiviert.



### 5.1.7 Tipps mit Scripts

- Um eine 'cmd.exe' Console zu verlassen, genügt das Kommando 'x'. Das Script x.bat wird gestartet, es enthält nur den Befehl exit.
- Um ein laufendes Programm oder Script gewaltsam abzubrechen, kann Strg-C gedrückt werden.
- Ein Script besteht aus mehreren Kommandos. Wurde ein Kommando nicht erfolgreich ausgeführt, kann das Script abgebrochen und ein Fehler angezeigt werden.

```
@echo off
```

```
rtcmd pb -i s=*USR\Hans\Eigene Dateien\data tf30=*NET\*ARCH\*  
IF %ERRORLEVEL% NEQ 0 exit %ERRORLEVEL%
```

```
rtcmd pb -i s=*USR\Maria\Eigene Dateien\data tf30=*NET\*ARCH\*
```

- Werden viele Programm gleichzeitig ausgeführt, empfiehlt sich die unsichtbare Console. Die Überwachung der Ausgabe kann bei Bedarf durch Öffnen der Protokolldateien in `RT_LOG` erfolgen. Console-Editor schaltet automatisch in den Überwachungsmodus, solange ein Protokoll nicht beendet ist.

## 5.2 Command Line

Editor, öffnet eine Datei:

```
c_e [-CONTROL] [PATH] [FILE]
```

Console, startet ein Programm auf dem lokalen- oder einem Netzwerk-Rechner:

```
c_e [-CONTROL] [CREDENTIALS] [(D,T) SCHEDULE] [PATH\] [FILE] [PARAMETER] ...
```

```
c_e
```

Öffnet eine neue Textdatei.

Um Console-Editor mit administrativen Rechten zu starten, muss ab Vista™ und bei eingeschalteter Benutzerkontensteuerung das Kommando `c_u` oder `c_a` anstatt `c_e` verwendet werden. Die Command Line bleibt dabei identisch.

Benutzerkonten-Steuerung		
	Administrator	eingeschränktes Konto
<b>c_e</b>	keine administrativen Rechte.	keine administrativen Rechte.
<b>c_u</b>	administrative Rechte.	keine administrativen Rechte.
<b>c_a</b>	administrative Rechte.	administrative Rechte.

`c_u * x`, oder `c_a * x` startet ein beliebiges Programm `x` mit den entsprechenden Rechten und kommt sofort zurück.

### 5.2.1 CONTROL

Optionen, Kombination aus folgenden Buchstaben:

Editor	
<b>b Binary</b>	Öffnet FILE im Hexadezimalformat, alle Zeichen werden als Zahlen im 16er System angezeigt.
<b>o OEM</b>	Öffnet FILE mit dem OEM Zeichensatz. Der OEM Zeichensatz wird oft von Kommandozeilenprogrammen benutzt und unterscheidet sich bei Umlauten vom ANSI Zeichensatz, der von Windows® benutzt wird.
<b>r Read Only</b>	Öffnet FILE, so dass es nicht verändert werden kann.
<b>v View</b>	Überwacht eine Log-Datei.
Console	
<b>x Execute</b>	Startet FILE mit allen PARAMETERN. Ohne FILE wird 'ComSpec' gestartet. Wenn <code>Exit</code> gleich Null ist (ERFOLG), wird das Fenster geschlossen.
<b>h Hidden</b>	Startet FILE unsichtbar mit allen PARAMETERN. Wenn <code>Exit</code> ungleich Null ist (VERSAGEN), wird ein Fehler gemeldet.
<b>c Clean</b>	Zeigt keine PARAMETER in der Titelleiste der Console und in Fehler- und Erfolgsmeldungen an. Sinnvoll, wenn ein Passwort in der Command Line angegeben ist. Von der Console abgefragte Passworte werden nie angezeigt.
<b>e Exit</b>	Beendet ein laufendes Programm ohne Nachfrage, wenn ein Benutzer abgemeldet oder ein Consolen-Fenster geschlossen wird.
<b>i Integrate</b>	Für Scripts, unterdrückt alle Meldungen und schließt das Consolen-Fenster nach Beendigung des Programmes.
<b>g Go</b>	Put computer on standby.
<b>l Logoff</b>	Logoff the current user.

These commands will only be processed on SUCCESS or without FILE.

<b>s Start</b>	Restart this computer.	
<b>t Terminate</b>	Terminate this computer.	
	<b>Console sichtbar</b>	<b>Console unsichtbar</b>
<b>p Pause</b>	Das Consolen-Fenster bleibt sowohl bei ERFOLG als auch bei VERSAGEN geöffnet.	Meldung bei ERFOLG und bei VERSAGEN.

```
c_e -ht
```

Schaltet den Rechner aus.

## 5.2.2 CREDENTIALS

```
\\[MACHINE] : [USER] : [PASSWORD]
```

Startet eine Console oder ein Programm unter einem anderen Benutzerkonto oder auf einem anderen Rechner im Netzwerk. Die Anmeldung an einem fremden Rechner erfordert immer ein Benutzerkonto mit den selben Anmeldedaten.

Um die Remote-Funktion zu nutzen gibt es 2 Möglichkeiten:

1. Entweder, benötigen Sie administrative Rechte. ADMIN\$ und IPC\$ muss auf dem Zielrechner freigegeben sein. Bei Windows® XP-Home scheint dies nicht möglich zu sein. Ab Vista™ ist die Freigabe auch bei Home-Versionen voreingestellt. Die Benutzerkontensteuerung muss für das Administrator Konto auf dem Zielrechner ausgeschaltet sein. Dies ist die Voreinstellung für das eingebaute Administrator-Konto.

2. Oder, der Backup-Service muss auf dem Zielrechner installiert sein (Einstellungen->Setup All).

Ist MACHINE leer, wird der lokale Rechner ausgewählt.

Wird USER leer gelassen, wird das System-Konto ausgewählt. Vom System-Konto kann nicht auf das Netzwerk zugegriffen werden, ansonsten besitzt es alle administrativen Rechte. Sind Sie selbst Administrator, können Sie sich ohne Passwort anmelden, wenn nicht, muss der Backup-Service installiert sein, und Ihr Administrator muss ein Backup-Passwort vergeben haben (Einstellungen->Backup Passwort).

Wird PASSWORD leer gelassen (empfohlen), dann wird das Passwort bei Bedarf abgefragt.

Die Kommunikation zu einem anderen Rechner im Netzwerk wird mit DES 1024 und AES 256 verschlüsselt.

<b>\\</b>	lokale Console mit System-Rechten (kein Netzwerk).
<b>\\Pc</b>	Console auf Pc mit System-Rechten (kein Netzwerk).
<b>\\Pc:Hans</b>	persönliche Console auf Pc.
<b>\\:Hans</b>	persönliche Console auf lokalem Rechner.

```
c_e \\Pc
```

Startet cmd.exe auf Pc.

```
c_e \\Pc rtcmd ir -o1 s=C:*ARCH* t=*
```

Stellt Pc mit Dialog wieder her.

```
c_e \\Pc c_u * c_e -his rtcmd ir -i s=C:*ARCH* t=*
```

Stellt Pc ohne Dialog von der neusten Sicherung wieder her und kommt sofort zurück. Startet Pc nach der Wiederherstellung neu. Alle Protokolle werden auf Pc erstellt.

## 5.2.3 [D,T]SCHEDULE

**Wiederholfunktion**, startet alle SCHEDULE Sekunden eine sichtbare oder unsichtbare Console. Die Wiederholung wird abgebrochen, wenn Exit ungleich Null ist (VERSAGEN).

```
c_e -h 14400 *DOC\ rtcmd pb -i s=data tf30=*HD*ARCH* tof30=*NET*ARCH*
```

Sichert den Ordner data alle 4 Stunden im Hintergrund.

Der Vorteil von SCHEDULE gegenüber dem [Windows® Zeitplandienst](#) ist, dass der Zeitzähler von SCHEDULE nur weiter läuft, wenn der jeweilige Benutzer angemeldet ist. Der Zeitzähler wird aber nicht durch Install-Restore unterbrochen oder wenn verschiedene Installationen oder Betriebssysteme benutzt werden.

SCHEDULE eignet sich hervorragend für die regelmäßige automatische Sicherung von wichtigen Anwenderdaten.

Beachten Sie die Beispiel-Scripts im Ordner 'Scripts\AutoBackup'.

**Tageskonto(D)**, begrenzt die tägliche Anmeldezeit auf D SCHEDULE Sekunden.

```
c_e -ht D1800
```

Nach einer täglichen Anmeldezeit von 30 Minuten wird der Computer ausgeschaltet.

Der Benutzer kann sich mehrmals täglich anmelden, hat aber insgesamt nur 30 Minuten Computerzeit.

**Zeitsparkasse(T)**, begrenzt die durchschnittliche tägliche Anmeldezeit auf T SCHEDULE Sekunden.

Effektiver Schutz gegen Computer-Missbrauch bei Kindern.

```
c_e -ht T600
```

Der Benutzer spart jeden Tag 10 Minuten Computerzeit. Nur wenn das Konto der Zeitsparkasse im Plus ist kann er angemeldet werden.

```
SET KEY=HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
reg add %KEY% /v Zeitsparkasse /d "%RT%\c_e.exe -hl T600" /f
```

Dieses Script installiert die Zeitsparkasse für den aktuellen Benutzer.

## 5.2.4 PATH

PATH ist der Ordner in dem eine Datei bearbeitet, ausgeführt oder überwacht werden soll. PATH kann [Pfadjoker](#) enthalten und muss immer mit einem '\' enden.

```
c_e *DOC\ Notizen.txt
```

Bearbeitet das Dokument 'Notizen.txt' im Ordner 'Eigene Dateien' bzw. 'Dokumente'

```
c_e -x *DOC\
```

Startet das Windows® Kommandozeilenprogramm 'cmd.exe' im Ordner 'Eigene Dateien' bzw. 'Dokumente'.

## 5.2.5 FILE

FILE ist eine Datei, die zum Bearbeiten, Überwachen oder zum Ausführen geöffnet wird.

```
c_e Notizen.txt
```

Öffnet die Datei Notizen.txt zum Bearbeiten.

Wurde eine Datei vor dem Öffnen mit Console-Editor von einem anderen Programm geöffnet, dann wird automatisch in den Überwachungsmodus geschaltet und das Ende der Datei angezeigt.

```
c_e %SystemRoot%\pfirewall.log
```

Öffnet und überwacht das Sicherheitsprotokoll der Windows® Firewall. Das Sicherheitsprotokoll muss vorher im Eigenschaften-Fenster der Firewall eingeschaltet werden.

```
c_e -xp rtcmd
```

Startet rtcmd ohne Parameter.

## 5.2.6 PARAMETER

Ist FILE ein Programm oder Script, das gestartet werden soll, dann können beliebig viele PARAMETER übergeben werden.

```
c_e -xp rtcmd pb -nm s=Briefe
```

RtCmd wird mit den Parametern pb, -nm und s=Briefe gestartet.

Alles, was zwischen Fragezeichen steht, wird beim Start der Console ersetzt:

<b>?xxxx?</b>	Offene Parametereingabe
<b>??xxxx??</b>	Einfache Passworteingabe

??x??

Doppelte Passworteingabe

```
c_e -xp rtcmd pb p=??Zip Passwort?? s=Briefe
```

Beim Starten der Console wird ein doppeltes Passwort abgefragt. Sind die Passworte nicht identisch, wird die Abfrage wiederholt.



## 6: Tools

### 6.1 Benutzer-Konten

#### 6.1.1 account, erstellt Benutzer-Konten

```
rtcmd account CREDENTIALS [GROUP] ...
```

**Account** erstellt einen Benutzer, setzt die Mitgliedschaft und meldet ihn an, um sein Profil zu erzeugen.

CREDENTIALS wird im [Standard-Format](#) angegeben.

```
rtcmd account \\:Hans:uhmrvttkv11kq43t Benutzer
```

Erstellt ein Benutzer-Konto für Hans und setzt ein sicheres 16-Stelliges Passwort. Hans wird Mitglied der Gruppe 'Benutzer'. Ist das Konto bereits vorhanden, so wird das Passwort und die Mitgliedschaft überprüft und ggf. berichtigt.

Das Account Kommando kann genutzt werden um in kleinen Netzwerken ohne [Active-Directory](#) einen Benutzer-Stamm automatisiert auf allen Rechnern bereit zu stellen.

#### 6.1.2 Backup-Service, Dienst für eingeschränkte Benutzer-Konten

Der Backup-Service ist ein Dienst, der beim Reuschools Setup-Assistenten ausgewählt werden kann. Dieser Dienst hat die Aufgabe auch Benutzern, die keine administrative Rechte haben, Backups zu ermöglichen, die erweiterte Rechte benötigen:

**Private-Backup**, jeder Benutzer kann ein Backup von einem Ordner erstellen, solange keine darin enthaltene Dateien gerade geöffnet sind. Besonders gestartete Datenbanken haben jedoch ständig geöffnete Dateien. Um diese in einem Zustand zu sichern, von dem die Datenbank wieder korrekt hergestellt werden kann wird der [Windows® Schattenkopierer](#) benötigt. Dieser Dienst erfordert administrative Rechte.

Da manche E-Mail Programme ihre Daten in Datenbanken ablegen und diese Programme oft schon mit der Benutzer-Anmeldung gestartet werden, ist es möglich, dass ein Anwender ohne administrative Rechte seine E-Mails nicht sichern kann.

Wurde der Backup-Service installiert, so übernimmt dieser automatisch das Starten des Schattenkopierers, sodass diesbezüglich keine Probleme mehr zu erwarten sind.

**Private-Restore**, jeder Benutzer kann einen Ordner mit Private-Restore wiederherstellen, solange keine darin enthaltenen Dateien geöffnet sind. Um geöffnete Dateien wiederherzustellen werden diese in eine Liste eingetragen, die beim nächsten Start des Rechners abgearbeitet wird. Diese Liste kann aber wiederum nur mit administrativen Rechten bearbeitet werden. Auch hier übernimmt der Backup-Service automatisch die Eintragung.

**Install-Backup**, ein Benutzer mit eingeschränkten Rechten kann kein Backup des Windows®-Systems durchführen. Ist der Backup-Service installiert, so kann der Administrator zusätzlich ein [Backup-Passwort](#) vergeben. Mit Hilfe dieses Passwortes können auch Benutzer mit eingeschränkten Rechten das komplette Windows-System sichern. Dabei wird Zugriff auf das lokale System-Konto gewährt. Mit diesem Konto kann nur auf die lokale Festplatte, nicht aber auf das Netzwerk zugegriffen werden.

**Install-Restore**, angenommen ein Benutzer mit eingeschränkten Rechten erhält ein E-Mail, das sich nach dem öffnen als äußerst verdächtig erweist. Der Benutzer bemerkt, dass sich etwas von selbst installiert und versucht deshalb den Vorgang sofort abzubrechen und das E-Mail zu löschen. Doch das ist schon zu spät. Ein Überwachungs-Trojaner kann sich ohne Probleme auch in ein Benutzer-Konto mit eingeschränkten Rechten installieren.

Der Benutzer hat jetzt ein schlechtes Gewissen und hofft, dass nichts passiert ist. Möglicherweise hat er sein privates E-Mail-Konto während der Arbeitszeit abgerufen, weshalb er versucht diesen Vorfall zu verheimlichen.

Wurde der Backup-Service installiert und ein Backup-Passwort vergeben, so kann der Anwender selbst und ohne Aufsehen den Rechner mit Hilfe von Install-Restore desinfizieren, um so größeren Schaden wie z.B. Industriespionage abzuwenden.

#### 6.1.3 efskey, generiert Schlüssel für das Datei-System

```
rtcmd efskey CREDENTIALS [-i] [-KEYLENTH] [PFXPASSWROD]
```

**Efs Key** generiert bzw. überprüft einen EFS Schlüssel aus dem aktuellen Verzeichnis.

CREDENTIALS wird im [Standard-Format](#) angegeben.

Generiert ein EFS-Zertifikat für das angegebene Benutzerkonto. Das Zertifikat wird danach in das aktuelle Verzeichnis exportiert.

```
rtcmd efskey \\:Hans:uhmrvttkv11kq43t pfxgeheim
```

Für Hans wird ein Zertifikat erstellt mit dem er seine Dateien EFS-verschlüsseln kann. Das Zertifikat wird anschließend in das aktuelle Verzeichnis unter dem Namen 'Hans.pfx' importiert.

Ist im aktuellen Verzeichnis ein Zertifikat mit dem angegebenen Benutzernamen vorhanden, so wird dieses verwendet.

Achtung, stellen Sie sicher, dass ein Benutzer auf allen Rechnern immer das selbe Zertifikat einsetzt, und dass dieses durch ein sicheres Backup gesichert ist. Ansonsten kann es zu Daten-Verlust kommen.

Leider ist es möglich in ein Benutzer-Konto mehrere EFS-Zertifikate zu importieren. Welches Windows® für die Verschlüsselung verwendet ist dann nicht mehr eindeutig. Aus diesem Grund sollten alle Benutzer-Konten mit einem gesicherten Zertifikat ausgestattet werden.

Das Kommando 'efskey' stellt sicher, dass nur ein Zertifikat zur Verfügung steht. Entspricht dies nicht dem im aktuellen Pfad bereitgestellten, so wird mit einer Fehlermeldung abgebrochen.

Selbstverständlich sollten alle Scripts, die folgende Kommandos mit der Angabe Passworten nutzen, selbst EFS verschlüsselt und somit nur vom Administrator lesbar sein:

rtcmd account
rtcmd efskey
rtcmd profiler
rtcmd encrypt
rtcmd decrypt

Nutzen Sie Private-Backup und Private-Restore um verschlüsselte Ordner mit Scripts und Zertifikaten vertraulich auf andere Rechner zu übertragen.

Vorteilhaft ist ein Backup im [RAW-Format](#). Demarkieren Sie hierzu im Assistenten die Option 'EFS-Verschlüsselung'. Wenn nicht der Haupt-Ordner sondern nur ein Unter-Ordner als EFS-verschlüsselt markiert ist kann die verschlüsselte Wiederherstellung auch so auf Windows® Home Versionen durchgeführt werden.

#### 6.1.4 password, generiert Passworte

```
rtcmd password [NUMBER]
```

**Password** generiert zufällige sichere Passworte aus verwechslungsfreien Buchstaben.

NUMBER gibt an, wie viele 16-stellige Passworte generiert werden sollen. Wird NUMBER weggelassen, so werden 100 Passworte generiert.

Die Zeichenauswahl für Passwortzeichen ist so gewählt, dass Verwechslungen ausgeschlossen sind. Es werden keine Großbuchstaben verwendet, um eine sehr schnelle Passworteingabe zu ermöglichen.

```
123456789abcdefghijklmnopqrstuvwxyz"
```

Ein Zeichen entspricht 5 Bit. Ein 16-stelliges Passwort somit aus 80 Bit. Um ein 16-stelliges Passwort zu erraten, muss ein Angreifer bis zu 1.208.925.819.614.629.174.706.176 verschiedene Passworte überprüfen. Ein gutes Passwortknackprogramm kann pro Sekunde ca. 10 Mio. Passworte ausprobieren. Das Erraten des Passwortes dauert somit im Durchschnitt 1.943.360.692 Jahre.

```
start rcmd password
```

Wird vor dem Kommando der Start Befehl eingegeben, dann werden die generierten Passworte in einem Dos-Fenster angezeigt und nicht protokolliert.

Ein Windows® Benutzerpasswort, das auch für die Sicherheit von [EFS](#) entscheidend ist, muss aus mindestens 15 Zeichen bestehen! Ein 12-stellige Zufallspasswort kann dazu mit 3 gleichen Buchstaben verlängert werden. Siehe hierzu Microsoft®, Hilfe und Support, Artikel 299656, Methode 3:

[So verhindern Sie, dass Windows LAN Manager Hashwerte Ihres Kennworts in Active Directory und der lokalen SAM-Datenbank speichert.](#)

So funktioniert der Zufallsgenerator:

- Die hochauflösende Uhr des Computers (genauer als eine Millionstel Sekunde) wird 32768 mal abgefragt und die unteren 32 Bit werden gespeichert.
- Die so gewonnenen Daten werden zipkomprimiert.
- Aus den komprimierten Daten wird ein 32 Bit CRC Wert errechnet.
- Aus dem CRC Wert werden 4 Stellen eines Passwortes errechnet.

#### 6.1.5 profiler, verschiebt Ordner für regelmäßige Backups

```
rtcmd profiler [CREDENTIALS] [-nd] [SOURCE] [*] [TARGET]
```

**Profiler** ist ein Werkzeug zum Verschieben wichtiger Ordnern z.B. nach 'Eigene Dateien'.

CREDENTIALS wird im [Standard-Format](#) angegeben.

Mit dem Profiler kann beim Einrichten des Windows® Systems ein persönlicher Daten-Ordner geschnürt werden. Dieser Daten-Ordner ermöglicht es zu jeder Zeit von einem Rechner zu einem anderen zu wechseln, und dort alle Daten verfügbar zu haben um sofort weiterarbeiten zu können.

Ein typisches Szenario ist der wechselseitige Einsatz eines PCs am Arbeitsplatz und der eines Notebooks für die Reise. Ebenso muss an den plötzlichen Ausfall eines Rechners gedacht werden, der im Notfall ohne Zeitverlust zu ersetzen ist. Dabei sollte ein Wechsel auch zwischen verschiedenen Sprach- und Systemversionen von Windows® ohne Probleme möglich sein.

Alle Office Dokumente können vom Anwender ohne Konfiguration innerhalb des Daten-Ordners gespeichert werden. Dieser wird regelmäßig mit Private-Backup gesichert wodurch jederzeit frühere Versionen eines Dokuments oder Emails gesichtet bzw. wiederhergestellt werden können.

Oft sind Windows®-Systeme so konfiguriert, dass jeweils das gesamte Benutzer-Profil (C:\Benutzer\hans) für ein Backup ausgewählt wird.

<b>Nachteile durch ein Backup des gesamten Benutzer-Profils</b>
Ein Benutzer-Profil kann komplett installierte Trojaner enthalten, die so auf einen anderen Rechner übertragen werden werden.
Das Benutzer-Profil enthält temporäre Dateien wie z.B. die besuchten Internet-Seiten. Solche Daten können gigantische (Gigabyte) Ausmaße annehmen und müssen nicht gesichert werden.
Der Umzug auf ein anderes System ist nicht ohne Probleme möglich.

Deshalb lohnt sich der einmalige Konfigurations-Aufwand für einen Daten-Ordner.

**Funktion:** Der Profiler verschiebt die oder den Ordner in den ausgewählten Daten-Ordner. Anstelle des Original-Ordners wird eine Verknüpfung (Reparse-Point) gesetzt. Dadurch sind keine weiteren Einstellungen an dem jeweiligen Programm notwendig. Dieses glaubt weiterhin seine Daten in den Original-Ordner zu schreiben, schreibt aber in Wirklichkeit in den Datenordner. Der Profiler kann mehrfach aufgerufen werden ohne dass es zum Datenverlust im Datenordner kommt. Ist eine Datei im Datenordner bereits vorhanden, so wird diese nicht ersetzt.

Der Profiler wird im Arbeits-Alltag nicht benötigt. Deshalb gibt es beim Reushtools Setup Assistenten keine entsprechende Option. Der Profiler kann von einer Console gestartet werden. Hier sind mehrere Szenarien:

- **Typische Ordner verschieben:** Oft ist es problematisch herauszufinden, wo genau manche Programme ihre Daten wie z.B. Emails abspeichern. Deshalb kann der Profiler von einer beliebigen Console (z.B. Start\Programme\Reushtools\Console) für typische Ordner aufgerufen werden:

```
rtcmd profiler *
```

Der Assistent erscheint und der Anwender kann aus verschiedenen Ordnern auswählen:

<b>Typische Ordner mit wichtigen Daten</b>
Favoriten
Desktop
Windows Mail
Kontakte
Office Outlook
Skype
Kalender

- **ausgewählte Ordner verschieben:** Ist ein wichtiger Ordner nicht in obiger Tabelle enthalten, so muss dieser zuerst gefunden und dann manuell ausgewählt werden.

Wurde beim Reushtools Setup die Console ausgewählt, so klicken Sie mit der rechten Maus-Taste auf den wichtigen Ordner und wählen Console. Um den Assistenten zu starten genügt das Kommando:

```
rtcmd profiler
```

Um den Vorgang noch einfacher zu gestalten, kann ein Eintrag im Kontext-Menü von Ordnern ein:

```
Scripts\UserAccounts\ProfilerOn
```

bzw. ausgeschaltet werden.

```
Scripts\UserAccounts\ProfilerOff
```

- **Fremde Benutzer konfigurieren:** Der Profiler eignet sich auch für die automatisierte Benutzerkonfiguration in kleinen Netzwerken ohne Active-Directory. Werden mit dem Start des Profilers Anmeldedaten (**CREDENTIALS**) angegeben, kann der Assistent für einen fremden Benutzer gestartet werden:

```
rtcmd profiler \\:Hans *
```

Wird ein wichtiger Ordner (SOURCE) und ein Daten-Ordner (TARGET) in der Command Line angegeben, arbeitet der Profiler ohne Interaktion. Ein solches Kommando kann in einem Benutzer-Konfigurations-Scrip genutzt werden, das auf mehreren Rechnern eines kleinen Netzwerkes ausgeführt wird:

```
rtcmd profiler \\:Hans:%PASSWORD% *USR\Hans\Contacts *DOC\data
```

Für den Profiler stehen zusätzliche benutzerabhängige Variablen zur Verfügung:

Variable	Beispiel
*Home	C:\Users\Hans
*Favorites	C:\Users\Hans\Favoriten
*Desktop	C:\Users\Hans\Desktop
*AppData	C:\Users\Hans\AppData\Roaming
*LocAppData	C:\Users\Hans\AppData\Local

Obiges Kommando kann damit auch so geschrieben werden:

```
rtcmd profiler \\:\Hans:%PASSWORD% *HOME\Contacts *DOC\data
```

#### - Temporären Ordner von einem Backup ausschließen:

Sollen in einem Ordner temporäre Dateien von einem Backup ausgeschlossen werden, kann der Profiler auch in umgekehrter Richtung genutzt werden. Verschieben Sie den Ordner, der nicht in ein Backup integriert werden soll, in einen temporären Ordner außerhalb ihres Windows® z.B. nach C:\temp.

Um den Assistenten zu verwenden kann wieder das Kommando:

```
rtcmd profiler
```

aufgerufen werden, wenn der Pfad auf den Quellordner zeigt.

#### No Delay (-nd):

Wird ein Ordner verschoben, dessen Dateien gerade benutzt werden, so wird der Vorgang normalerweise bei der nächsten Benutzer-Anmeldung durchgeführt. Die -nd Option verhindert dies und führt zum Abbruch und zur Fehlermeldung des Profilers.

### 6.1.6 Zeitsparkasse, Hilfsprogramm gegen PC-Abusus

**Problemstellung**, die Zeitsparkasse wurde für geplagte Eltern entwickelt, deren Sprösslinge zu viel Zeit am PC und zu wenig mit Hausaufgaben oder anderen Pflichten verbringen. Auch wenn sich das Problem mehr und mehr auf den mobilen Bereich verlagert bleibt doch der PC mit Chat und Spielen in vielen Familien relevant.

Andere Systeme, wie z.B. die Begrenzung der täglichen Computer-Zeit haben sich in der Praxis nicht ausreichend bewährt. Besonders die Beschränkung der täglichen Zeit führt dazu, dass Spiel oder Arbeit unterbrochen werden, um die vorhandene Zeit auszunutzen, da diese nicht auf den nächsten Tag aufgehoben werden kann. Somit wird ausgerechnet das erreicht, was eigentlich vermieden werden soll: Das Kind oder der Jugendliche richtet seine Zeit-Planung weitgehend nach dem Medien-Konsum.

Vor diesem Hintergrund wurde das Konzept der Zeitsparkasse entworfen und ausgiebig in der Praxis getestet. Die Zeitsparkasse spart jeden Tag automatisch die vorgegebene Computerzeit, egal ob sich der Benutzer anmeldet oder nicht.

So kann der Anwender z.B. seine Computerzeit auf das Wochenende aufsparen um dann ausgeprägtere Computersitzungen vorzunehmen. Ebenso können Geschwister, von denen jeder ein eigenes Zeitkonto besitzt, ihre Zeit gemeinsam nutzen, um z.B. einen Filme-Abend am PC zu organisieren.

Weitere Erfahrungen wurden mit der Beschränkung von negativen oder schädlichen Inhalten aus dem Internet gemacht. Jegliche Beschränkung irgendwelcher Inhalte führte letztendlich zum Reiz des Verbotenen. Ist eine Seite auf dem häuslichen PC gesperrt so versuchen Kinder und Jugendliche diese vom PC eines Freundes zu besuchen. Mit der Zeitsparkasse wird die Gesamtzeit vor dem PC eingeschränkt, was dazu führt, dass der Anwender selbst lernt zu entscheiden, welche Inhalte wertvoll und sinnvoll für ihn sind.

**Funktion**, die Zeitsparkasse wird automatisch bei der Anmeldung eines Benutzers gestartet. Kurz nach der Anmeldung erscheint ein Fenster das anzeigt, wie viel Zeit der Benutzer angespart hat. In der Startleiste erscheint ein Icon über das der Benutzer die verbleibende Zeit überprüfen kann. Ist weniger als 1. Minute auf dem Zeitkonto erscheint ein Warnfenster. Nachdem die Zeit abgelaufen ist wird der Benutzer entweder abgemeldet oder der PC ausgeschaltet. Die Zeitsparkasse erhebt nicht den Anspruch einbruchssicher zu sein. Ein Computer-Experte könnte sie leicht manipulieren oder deaktivieren. Deshalb sollte das notwendige Vertrauen zum Anwendender vorhanden und um Verständnis und Akzeptanz einer eingeschränkten Computer-Nutzung geworben werden. Sprechen Sie mit Ihrem Kind vor der Anschaffung seines eigenen PCs über das Thema Medienkompetenz und die Einrichtung einer Zeitsparkasse.

**Kosten**, die Zeitsparkasse ist im Reushtools Komplettpaket enthalten. Reushtools ist nicht kostenlos. Beim Einsatz der Zeitsparkasse gibt es jedoch keinerlei Einschränkung. Auch nach dem Ablauf der 6 monatigen Testperiode kann die Zeitsparkasse weiterhin ohne gültige Lizenz genutzt werden.

**Installation**, starten Sie einfach das Installations-Programm auf der Reushtools-Download-Seite. Bei den Installations-Optionen markieren Sie ausschließlich das Kästchen 'Scripting'. Nach dem Abschluss der Installation öffnen Sie den Ordner 'Scripts' (Start->Programme->Reushtools->Scripts). Die Zeitsparkasse wird mit dem sich selbst erklärenden Script 'UserAccount\Zeitsparkasse.cmd' eingerichtet.

## 6.2 Datei-System

### 6.2.1 access, setzt Berechtigungen

```
rtcmd access DIRECTORY
```

**Access Directory** setzt die Berechtigungen für gesperrte Objekte auf Administrator.

Access erzwingt den Zugriff auf einen Ordner und dessen Inhalt. Die [Berechtigungen](#) werden bei Bedarf entsprechend verändert.

### 6.2.2 acl, zeigt Berechtigungen

```
rtcmd acl DIRECTORY|FILE
```

**Show Acl** zeigt die Berechtigungen für eine Datei oder ein Verzeichnis im 'Security Descriptor String Format'.

Access Control List zeigt die [Berechtigungen](#) im [Security Descriptor String Format](#) an.

### 6.2.3 tree, shows a file tree

```
rtcmd tree
```

**File-Tree** shows a tree of all files on the machine and the network.

### 6.2.4 cleantree, erstellt einen leeren Ordner

```
rtcmd cleantree DIRECTORY
```

**Clean Tree** erstellt ein Verzeichnis, bzw. löscht dessen Inhalt.

Kann eine Datei nicht gelöscht werden führt dies zur Fehler-Meldung und zum Abbruch.

### 6.2.5 decrypt, entschlüsselt ein Objekt

```
rtcmd decrypt [CREDENTIALS] FILE|DIRECTORY[\\]
```

**Decrypt** entschlüsselt eine Datei oder einen Ordner mit EFS.

CREDENTIALS wird im [Standard-Format](#) angegeben. Wird DIRECTORY mit einem '\\' beendet, so wird der Ordner und sein Inhalt entschlüsselt.

### 6.2.6 delfile, löscht eine Datei

```
rtcmd delfile FILE
```

**Delete File** löscht eine Datei.

### 6.2.7 deltree, löscht einen Ordner

```
rtcmd deltree DIRECTORY
```

**Delete Tree** löscht einen kompletten Ordner.

```
rtcmd deltree "C:\System Volume Information"
```

Entfernt das Verzeichnis 'C:\System Volume Information'.

Kann eine Datei oder Ordner nicht gelöscht werden, so wird versucht dies beim nächsten Neustart zu erledigen.

### 6.2.8 encrypt, verschlüsselt ein Objekt

```
rtcmd encrypt [CREDENTIALS] FILE|DIRECTORY[\\]
```

**Encrypt** verschlüsselt eine Datei oder einen Ordner mit EFS.

CREDENTIALS wird im [Standard-Format](#) angegeben. Wird DIRECTORY mit einem '\\' beendet, so wird der Ordner und sein Inhalt verschlüsselt.

### 6.2.9 list, zeigt den Inhalt eines Ordners oder Laufwerks

```
rtcmd list [-n|-t|-s|-h] [DIRECTORY]
```

**List** erstellt eine Liste mit allen Dateien und Unterordnern eines Ordners oder eines Laufwerks. Dabei werden auch versteckte Objekte angezeigt. Es sind verschiedene Sortierungen wählbar.

<b>-n (default),</b>	alle Dateien und Ordner werden nach ihrem <b>Namen</b> sortiert.
----------------------	--

<b>-t</b>	alle Dateien und Ordner werden nach dem letzten Schreib- <b>Datum</b> sortiert.
-----------	---

<b>-s</b>	alle Dateien werden nach ihrer <b>Größe</b> sortiert.
<b>-h</b>	es werden nur <b>Hardlinks</b> und <b>Reparse-Points</b> angezeigt.

```
rtcmd list -t C:
```

Zeigt eine Liste mit allen Dateien und Ordnern des Laufwerks C:. Die Liste wird nach dem letzten Schreib-Datum sortiert.

### 6.2.10 seal, speichert eine Datei im RAW-Format

```
rtcmd seal FILE
```

**Seal** verschlüsselt eine Datei mit EFS und speichert sie im RAW-Format.

### 6.2.11 sopen, öffnet ein RAW-Archiv (.seal)

```
c_e -sopen SEALFILE
```

**Seal-Open** öffnet ein Zip-Archiv im **Seal-Format** mit dem Windows®-Explorer.

### 6.2.12 unseal, konvertiert eine Datei vom RAW-Format

```
rtcmd unseal FILE
```

**Unseal** liest eine Datei im RAW-Format und speichert sie als lesbare EFS-verschlüsselte Datei.

## 6.3 Windows® Registry

Für alle Registry-Tools werden administrative Rechte benötigt. Es werden auch versteckte oder gesperrte Informationen berücksichtigt.

BINLIN legt fest, nach wie vielen Zeilen die Ausgabe von binären Daten, die oft sehr lange sind, abgebrochen werden soll. Die Voreinstellung ist 40.

### 6.3.1 delkey, löscht einen Registry-Schlüssel

```
rtcmd delkey HKLM\KEY|HKCU\KEY
```

**Delete Key** löscht einen kompletten Schlüssel aus Windows(R) Registry.

### 6.3.2 hc, vergleicht zwei Hives

```
rtcmd hc [-BINARYLINES] HIVE1 HIVE2
```

**Hive Compare** vergleicht zwei Hives.

### 6.3.3 hs, zeigt einen Hive

```
rtcmd hs [-BINARYLINES] HIVE
```

**Hive Show** zeigt einen Hive.

### 6.3.4 ii, zeigt die Windows® Ordner

```
rtcmd ii
```

**Install Info** zeigt die Ordner der laufenden Windows(R)-Installation, EXIT ist die Windows(R)-Version.

Zeigt die Ordner der laufenden Installation, die Benutzerkennung und die Versionsnummer des Betriebssystems. **Exit** ist die Versionsnummer des Betriebssystems (5 für XP, 6 für Vista™).

### 6.3.5 rc, vergleicht die Registry

```
rtcmd rc [-BINARYLINES] [user|sam|security|software|system|components|bcd00000000]
```

**Registry Compare** vergleicht die aktuelle Windows(R) Registry mit der vorher exportierten.

**Registry Compare**, vergleicht **Hives** miteinander und gibt Unterschiede am Bildschirm aus. Wird HIVE1 und HIVE2 nicht angegeben, dann wird die gesamte Registry ein zweites Mal exportiert und die ersten **Hives** mit den zweiten verglichen. Dies ist sinnvoll, um zu untersuchen, was ein Programm in die Registry schreibt.

### 6.3.6 re, exportiert die Registry

```
rtcmd re [user|sam|security|software|system|components|bcd00000000]
```

**Registry Export** exportiert die Windows(R) Registry im Hive-Format.

**Registry Export**, exportiert die gesamte Registry in **Hives**.

### 6.3.7 rs, zeigt die Registry

```
rtcmd rs [-BINARYLINES] [user|sam|security|software|system|components|bcd00000000]
```

**Registry Show** zeigt die Windows(R) Registry.

**Registry Show**, gibt [Hives](#) am Bildschirm aus. Wird HIVE nicht angegeben, dann wird die gesamte Registry exportiert und ausgegeben.

## 6.4 Automatisierung

### 6.4.1 icons, zeigt alle Icons aus c\_e.exe und shell32.exe

```
c_e -icons
```

**Icons** zeigt ein Fenster mit einer Liste aller Icons die sich in c\_e.exe und shell32.exe befinden. Mit diesem Befehl können IconIds von Icons angezeigt werden. Verwenden Sie diese Nummern in den Befehlen mb\_ok, mb\_yes und mb\_yesno. Icons aus c\_e.exe erhalten ein negatives Vorzeichen. Ohne dieses Vorzeichen können alle Icons auch für das Kontext-Menü genutzt werden.

### 6.4.2 mb\_ok, Fenster mit OK

```
rtcmd mb_ok MESSAGE [HEADER] [ICON]
```

**Message-Box Ok** startet ein Benachrichtigungs-Fenster mit OK.

### 6.4.3 mb\_yes, Fenster mit Ja

```
rtcmd mb_yes QUESTION [HEADER] [ICON]
```

**Message-Box Yes** startet ein Benachrichtigungs-Fenster mit ja (EXIT 0).

### 6.4.4 mb\_yesno, Fenster mit Ja-Nein

```
rtcmd mb_yesno QUESTION [HEADER] [ICON]
```

**Message-Box Yes/No** startet ein Benachrichtigungs-Fenster mit ja (EXIT 0) und nein (EXIT 2).

Zeigt ein kleines Fenster mit QUEST und wartet bis der Benutzer entweder 'Ja' ([Exit 0](#)) oder 'Nein' (Exit -1) angeklickt hat.

### 6.4.5 sleep, wartet

```
rtcmd sleep SLEEPTIME
```

**Sleep** stoppt ein Script für SLEEPTIME Sekunden. Wartet SECONDS Sekunden und wird danach beendet.

### 6.4.6 start, startet einen Dienst

```
rtcmd start SERVICE
```

**Start Service** sendet das Start-Kommando an einen Dienst und wartet bis dieser gestartet ist.

Ein Dienst(Service) kann mit dem Kommando:

```
sc start SERVICE
```

gestartet werden. Nachteilig ist für Scripts, dass das 'sc' Kommando sofort zurückkommt nachdem es den Startbefehl an den Dienst weitergegeben hat, aber noch bevor der Dienst tatsächlich gestartet wurde.

Sind die nachfolgenden Scriptbefehle aber von dem Dienst abhängig kann:

```
rtcmd start SERVICE
```

bzw.

```
rtcmd stop SERVICE
```

verwendet werden. Diese Kommandos kommen erst zurück wenn ein Dienst gestartet bzw. beendet ist. [Exit](#) ist ungleich Null wenn der Befehl nicht innerhalb 1 Minute ausgeführt werden konnte.

### 6.4.7 stop, beendet einen Dienst

```
rtcmd stop SERVICE
```

**Stop Service** sendet das Stop-Kommando an einen Dienst und wartet bis dieser beendet ist.

## 6.4.8 wc, schließt ein Fenster

```
c_e -wc
```

**Window Close** schließt das aktuelle Windows®-Fenster.

## 6.4.9 zoom, verändert die Bildschirm-Auflösung

```
c_e -zoom(+|-)
```

**Zoom** vergrößert oder verkleinert die Bildschirm-Auflösung bei gleichem XY Verhältnis und gleicher Aktualisierungs-Rate.

Hotkey		
<b>c_e -zoom+</b>	AltGr+	Verkleinert die Bildschirmauflösung, das Bild wird hergezoomt.
<b>c_e -zoom-</b>	AltGr-	Vergrößert die Bildschirmauflösung, das Bild wird weggezoomt.
<b>c_e -wc</b>	F9	<b>Window Close</b> , schließt ein beliebiges Fenster. Bedenken Sie, wie viele rekursive motorische Gedanken Sie jeden Tag sinnlos verbrauchen, um mit der Maus das Kreuz zu suchen.

## 6.5 Reushtools Setup

### 6.5.1 backuppwd, setzt ein Backup-Passwort

```
rtcmd backuppwd [PASSWORD]|clear
```

**Backup-Password** setzt oder entfernt das Backup-Passwort, sollte im lokalen System-Konto ausgeführt werden. Das Backup-Passwort kann auch in einer Console unter dem Menüpunkt: 'Einstellungen->Backup Passwort' gesetzt werden. Ist die Console an einem Remote-Rechner angemeldet, so wird das Backup-Passwort am Remote-Rechner gesetzt.

### 6.5.2 liz, zeigt die Reushtools-Lizenz

```
rtcmd liz
```

**Lizenz** zeigt den Reushtools Lizenz-Status des laufenden Rechners. Des weiteren wird der Machine-Key des aktuellen Rechners angezeigt, der für den Erwerb einer gültigen Lizenz benötigt wird. Wenn Sie eine gültige Lizenz besitzen, ist **Exit 0**, wenn nicht -1. Dieser Befehl eignet sich für die automatische Überprüfung und Lizenzierung von mehreren Rechnern in einem Netzwerk.

### 6.5.3 noblub, deaktiviert eine Warn-Meldung

```
rtcmd noblub
```

**No Blub** deaktiviert die Warnmeldung des Sicherheits-Centers für den aktuellen Benutzer (ab Vista). kann auch manuell über: **Systemsteuerung->Sicherheit->Sicherheitscenter->Benachrichtigungsmethode** eingestellt werden.

### 6.5.4 path, erweitert die PATH Variable

```
rtcmd path sm|su|cm|cu PATH
```

**Path** aktualisiert die Umgebungsvariable PATH mit dem Parameter PATH. Das Sub-Kommando entnehmen Sie folgender Tabelle:

<b>sm</b>	Setup Machine, der Setup-Befehl wird für alle Benutzer ausgeführt.
<b>su</b>	Setup User, der Setup-Befehl wird für den aktuellen Benutzer ausgeführt.
<b>cm</b>	Clean Machine, der Deinstallations-Befehl wird für alle Benutzer ausgeführt.
<b>cu</b>	Clean User, der Deinstallations-Befehl wird für den aktuellen Benutzer ausgeführt.

### 6.5.5 rclick, registriert Einträge im Kontext-Menü

```
rtcmd rclick sm|su
```

**Right Click** registriert bzw. deregistriert die Datei RClick.dll für die Kontextmenü-Steuerung. Führen Sie diesen Befehl aus, nachdem Sie Einträge für das Kontext-Menü **registriert** oder **entfernt** haben. Dabei werden die notwendigen Einstellungen beim Windows®-Explorer vorgenommen, sodass der neue Kontext-Menü-Eintrag sofort erscheint. Sind alle Registrier-Einträge entfernt, so wird mit diesem Befehl die Kontext-Menü-Steuerung deinstalliert. Deshalb sind die Sub-Kommandos cm und cu hier nicht notwendig.



### 6.5.6 root, zeigt den Reushtools Installations-Pfad

```
rtcmd root
```

**Root** zeigt den Ordner aus dem RtCmd.exe gestartet wurde.

### 6.5.7 setup, registriert Reushtools

```
rtcmd setup sm|su|cm|cu [PATH]
```

**Setup** aktualisiert die Umgebungsvariablen PATH und RT für Reushtools und de-registriert RClick.dll und den Backup-Service

## 7: Appendix

### 7.1 Reushtools Konfiguration

#### 7.1.1 persönliche und systemübergreifende Installationen

Aus verschiedenen Gründen kann es sinnvoll sein Reushtools sowohl systemübergreifend als auch für den aktuellen Benutzer zu installieren. Wurde Reushtools z.B. für alle Benutzer nur mit der Funktion 'Backup Restore' installiert, so kann ein einzelner Anwender zusätzlich die Funktion 'Scripting' nutzen.

Persönliche Komponenten werden grundsätzlich nur für persönliche Installationen registriert. Nur so kann sichergestellt werden, dass die Komponenten auch wieder entfernt werden können, nachdem Reushtools für alle Benutzer deinstalliert wurde.

Bei Bedarf ist es möglich verschiedene Reushtools-Versionen nebeneinander zu nutzen. Wird eine neue Reushtools-Version zur Verfügung gestellt, während eine alte für alle Benutzer installiert ist, kann die neue zuerst nur vom aktuellen Benutzer eingesetzt werden.

Umgekehrt führt ein Upgrade für alle Benutzer nicht automatisch zum Upgrade für die persönliche Installation. Mit 'UpgradePersonal.exe' kann jedoch die persönliche Installation mit der systemübergreifenden aktualisiert werden.

#### 7.1.2 Konfiguration mit den Setup-Assistenten

Alle Komponenten, die während einer normalen Installation ausgewählt werden, können nachträglich von den Setup-Assistenten verändert werden.

<b>SetupAll.exe</b>	Die Komponenten-Auswahl gilt für alle Benutzer
<b>SetupPersonal.exe</b>	Die Komponenten-Auswahl gilt nur für den aktuellen Benutzer
<b>UpgradePersonal.exe</b>	Die Komponenten-Auswahl gilt nur für den aktuellen Benutzer. Dieser Assistent kopiert zusätzlich alle Reushtools-Dateien, die für alle Benutzer installiert wurden in ein persönliches Verzeichnis.

Die Setup-Assistenten können von einer Console unter dem Menü 'Einstellungen' aufgerufen werden. Auch das Deinstallations-Programm, das über die Systemsteuerung aufgerufen wird, startet den entsprechenden Setup-Assistenten. Um Reushtools zu deinstallieren müssen alle Komponenten abgewählt werden.

Das Installationsprogramm und die Setup-Assistenten führen nach der Konfiguration das Kommando 'rtcmd setup xx' aus. Dabei wird die Umgebungsvariable %RT% registriert, die auf den Installationsordner zeigt, um so z.B. schnell Verknüpfungen auf dem Desktop (%RT%\c\_e.exe) zu erstellen.

Außerdem wird die Umgebungsvariable %PATH% um den Installationsordner erweitert. Dadurch kann z.B. 'rtcmd' ohne Pfadangabe ausgeführt werden.

Anschließend wird geprüft ob Einträge im [Kontextmenü](#) gewünscht sind. Wenn ja, wird die Datei RClick.dll beim Explorer registriert damit die Einträge angezeigt werden.

Für den aktuellen Benutzer kann das Installationsprogramm aus Sicherheitsgründen vollständig blockiert werden:

```
reg add HKLM\Software\Reushtools /v AllowPersonal /t REG_DWORD /d 0 /f
```

#### 7.1.3 Bereitstellung ohne Installationsprogramm

Die in Reushtools enthaltenen Programme können ohne Installationsprogramm eingesetzt werden, indem die Programmdateien auf den entsprechenden Rechner kopiert werden.

Mit folgendem Kommando werden diese entpackt:

```
Reushtools_2.10.exe /X
```

Oder mit Pfad (Beispiel):

```
Reushtools_2.10.exe /X /D=C:\Reushtools
```

#### 7.1.4 Lautlose Installation

Reushtools kann mithilfe des Installationspakets lautlos installiert und konfiguriert werden:

```
Reushtools_2.10.exe /K=KOMPONENTS [/D=DIRECTORY]
```

#### KOMPONENTS

Das Installationsprogramm kann mehrfach aufgerufen werden, um nicht mehr benötigte Komponenten zu entfernen oder zusätzliche zu installieren.

KOMPONENTS ist eine Hexadezimalzahl die bestimmt, wie Reushtools installiert wird.

0x0001	<b>alle Benutzer</b>	Die Installation wird für alle Benutzer durchgeführt, mit '0' nur für den aktuellen.
0x0002	<b>Desktop Icon</b>	Verknüpfung auf dem Desktop: Erstellt ein Icon auf dem Desktop, um schnell auf die Funktionen von Reushtools zugreifen zu können.
0x0004	<b>Backup Restore</b>	Eintrag ins Kontextmenü: Startet mit einem Rechtsklick auf einen Ordner, ein Laufwerk oder den Computer die Datensicherung bzw. die Wiederherstellung.
0x0008	<b>Backup Service</b>	Dienst: Erlaubt auch Benutzern mit eingeschränkten Rechten, Dateien zu sichern, die gerade von einem anderen Programm geöffnet sind.
0x0010	<b>Zip_rt</b>	Eintrag ins Kontextmenü: Ermöglicht die schnelle Umwandlung eines Ordners in eine Zip-Datei und umgekehrt.
0x0020	<b>Console</b>	Eintrag ins Kontextmenü: Mit einem Rechtsklick auf einen Ordner, ein Laufwerk oder einen Rechner im Netzwerk wird eine Console gestartet.
0x0040	<b>Scripting</b>	Verknüpfung von Dateiendungen: '.bat' und '.cmd' Scripts werden nicht mehr im Dos-Fenster sondern in der Console ausgeführt. Zusätzlich werden <b>Input-Scripts</b> registriert. Achtung, die Console wird nach erfolgreichen .bat-Scripts automatisch geschlossen (c_e.exe -x), nach .cmd-Scripts bleibt die Console auch bei Erfolg geöffnet um das Protokoll zu betrachten (c_e.exe -xp).
0x0080	<b>Editor</b>	Verknüpfung von Dateiendungen: Textdateien mit der Endung '.txt' und '.log' werden nicht mehr mit Notepad sondern mit einem schnellen und professionellen Editor bearbeitet.
0x0100	<b>Startmenü</b>	Einträge in START->Programme->Reushtools: Schreibt nützliche Verknüpfungen in das Startmenü. Wird das Startmenü nicht geschrieben, enthält auch 'Desktop Icon' keine Einträge.
<b>Hotkeys</b>		
0x0200	<b>Zoom</b>	Ansicht vergrößern (AltGr+), Ansicht verkleinern (AltGr-). Ermöglicht die Verstellung der Bildschirmauflösung mit einer Tastenkombination.
0x0400	<b>Window-Close</b>	Schließt ein Windows® Programm auf Knopfdruck (F9).
0x0800	<b>Shutdown</b>	Benutzer abmelden (AltGr L), Rechner ausschalten (AltGr Ö), Rechner neu starten (AltGr Ä).
0x1000	<b>Command</b>	'cmd.com' für das Systemlaufwerk öffnen (AltGr C).
0x2000	<b>Text-Editor</b>	Text-Editor um Protokolle zu betrachten oder um Texte zu bearbeiten (AltGr T).
0x4000	<b>Archiv</b>	Öffnet das Hauptarchiv indem sich auch die Protokolle befinden (AltGr A).
0x8000	<b>Documents</b>	Öffnet den Ordner mit meinen Dokumenten (AltGr M).

```
Reushtools_2.10.exe /K=0x40
```

Nur die Funktion 'Scripting' wird für den aktuellen Benutzer installiert. Waren zuvor weitere Komponenten installiert, so werden diese entfernt.

#### DIRECTORY

Installationsordner. Ohne DIRECTORY wird in die Standardverzeichnisse installiert:

<b>alle Benutzer</b>	%ProgramFiles%\Reushtools
<b>aktueller Benutzer</b>	%Local AppData%\Reushtools

```
Reushtools_2.10.exe /K=0xFFFF /D=C:\Test
```

Reushtools wird in den Ordner C:\Test für alle Benutzer installiert und alle Komponenten ausgewählt.

Während der Installation wird im Installationsordner ein Protokoll (setup.log) erstellt, das anzeigt ob Dateien erst beim nächsten Neustart ersetzt werden.

Lautlose Deinstallation:

<b>SetupAll.exe /U</b>	Deinstallation für alle Benutzer
------------------------	----------------------------------

## 7.1.5 Upgrade

Ein Reuschtools Upgrade kann jederzeit mithilfe des neuen Installationsprogramms durchgeführt werden. Die alte Installation wird entfernt, auch wenn beim Upgrade ein anderes Installationsverzeichnis ausgewählt wird.

Das Installationsprogramm führt bei Bedarf einen Neustart des Explorers durch, um einen Neustart des Systems oder ein Abmelden des Benutzers zu vermeiden.

Kann eine Datei nicht ersetzt werden weil sie in Benutzung ist, fordert ein Dialogfenster zum Schließen des entsprechenden Programms auf, bzw. ermöglicht das Ersetzen beim nächsten Start des Rechners oder das Überspringen der Datei.

## 7.2 Einträge im Kontextmenü

### 7.2.1 RClick.dll

Klickt ein Anwender mit der rechten Maustaste auf ein Icon, so erscheint das Kontextmenü um diesem Icon eine Aufgabe zuzuordnen (z.B. Kopieren oder Drucken).

Ein ähnliches Kontextmenü kann durch einen Rechtsklick auf den Hintergrund eines geöffneten Ordners aufgerufen werden.

Mit der Kontextmenü-Erweiterung (RClick.dll) können beliebige Kommandos in das Kontextmenü eingetragen, und jedem Eintrag ein Symbol zur besseren Erkennung zugeordnet werden.

Während der Installation von Reuschtools können bei der Komponentenauswahl verschiedene Standardeinträge ausgewählt werden. Die Komponentenauswahl kann auch nachträglich von jeder Console unter 'Einstellungen->Setup Personal', oder 'Einstellungen->Setup All' verändert werden.

### 7.2.2 Iconklassen

RClick.dll unterscheidet folgende Iconklassen:

<b>Directory</b>	Ordnericon
<b>Background</b>	Ordnerhintergrund
<b>Drive</b>	Laufwerkicon, Laufwerkhintergrund
<b>LocalMachine</b>	Arbeitsplatz bzw. Computer
<b>Desktop</b>	Desktophintergrund
<b>Library</b>	'Eigene Dateien' bzw. 'Dokumente'
<b>RemoteMachine</b>	Rechner im Netzwerk
<b>Share</b>	Ordner im Netzwerk
<b>Archiv</b>	Icon von Zip- und Sealarchiven

### 7.2.3 Registrierung

Die Registrierung eines zusätzlichen Menüeintrags kann entweder mithilfe des Registriereditors oder eines Scripts erfolgen.

Der Registrierpfad ist davon abhängig, ob der Eintrag für alle Benutzer oder nur für den aktuellen gelten soll. Um Einträge für alle Benutzer zu registrieren sind administrative Rechte notwendig.

<b>alle Benutzer</b>	HKEY_LOCAL_MACHINE\Software\Reuschtools\RClick\KLASSE\MENÜ
<b>nur für mich</b>	HKEY_CURRENT_USER\Software\Reuschtools\RClick\KLASSE\MENÜ

Folgende Daten können von RClick.dll ausgewertet werden:

<b>(standard)</b>	REG_SZ	Command Line
<b>IconFile</b>	REG_SZ	Datei, in der sich das Symbol befindet, das mit dem Menüeintrag angezeigt werden soll.
<b>IconID</b>	REG_DWORD	Identifikationsnummer des Symbols.
<b>IconIndex</b>	REG_DWORD	Index des Symbols. Wurde 'IconID' registriert erübrigt sich 'IconIndex' und umgekehrt.
<b>Menu</b>	REG_DWORD	Beliebige Ordnungszahl, nach der die Reihenfolge der Menüeinträge ausgewählt wird. Einträge mit niedrigen Ordnungszahlen stehen weiter oben.

In der Command Line können spezielle Joker eingesetzt werden:

<b>*PATH</b>	Pfad des Ordners bzw. der Datei.
<b>*DIR</b>	Pfad ohne den Ordner bzw. die Datei.
<b>*FILE</b>	Dateiname ohne Pfad.
<b>*NAME</b>	Dateiname ohne Pfad und ohne Endung.
<b>*EXT</b>	Dateiendung.
<b>*MASCH</b>	Name eines Rechners oder eines Ordners im Netzwerk.

Nach der Registrierung muss 'rtcmd rclick su' für Einträge des aktuellen Benutzer oder 'rtcmd rclick sm' für Einträge aller Benutzer aufgerufen werden. Dieser Befehl meldet 'RClick.dll' beim Windows® Explorer an. Er ist nur notwendig, sofern vorher noch kein Eintrag für die jeweilige Iconklasse vorhanden war.

## 7.2.4 Beispiele

Alle Beispiele werden nur für das aktuelle Benutzerkonto registriert. Bitte beachten Sie auch das Script 'RClick.cmd' im Scriptordner.

### Kommentar-Feld eines Zip- oder Seal-Archives anzeigen:

```
set RCLICK=HKCU\Software\Reushtools\RClick\Archiv\ZipInfo
set CMD=c_a.exe -xp rtcmd zinfo \"*PATH\"
reg add %RCLICK% /ve /d \"%CMD%\" /f
RtCmd rclick su
```

Hier wird kein Menüsymbol registriert und keine Reihenfolge für den Eintrag festgelegt. Vor und nach \*PATH wurde \' gesetzt, um auch Dateinamen, die Leerzeichen enthalten, korrekt verarbeiten zu können.

### Remoterechner mit Install-Restore wiederherstellen und anschließend neu starten:

```
set RCLICK=HKCU\Software\Reushtools\RClick\RemoteMachine\Install-Restore
set REMOTE=c_a.exe -xps \\*MASCH
set CMD=rtcmd ir -id s=*HD\*ARCH\* t=*
reg add %RCLICK% /ve /d \"%REMOTE% %CMD%\" /f
reg add %RCLICK% /v IconFile /d "rtcmd.exe" /f
reg add %RCLICK% /v IconIndex /t REG_DWORD /d 2 /f
RtCmd rclick su
```

Hier wird eine anonyme Console gestartet. Um vom Remoterechner Zugriff auf das Netzwerk zu haben, kann die vierte Zeile durch

```
reg add %RCLICK% /ve /d \"%REMOTE%:%USERNAME% %CMD%\" /f
```

ersetzt werden. Die Variable %USERNAME% wird sofort beim ausführen dieses Scripts durch Ihren Namen ersetzt. Soll %USERNAME% hingegen erst durch das Kontextmenü ersetzt werden, um z.B. ein Kommando für alle Benutzer zu registrieren, so wird die Zeile zu:

```
reg add %RCLICK% /ve /d \"%REMOTE%:%USERNAME% %CMD%\" /f
```

### Überprüfen des Lizenzstatus eines Remoterechners:

```
set RCLICK=HKCU\Software\Reushtools\RClick\RemoteMachine\Lizenzstatus
set REMOTE=c_a.exe -xp \\*MASCH
set CMD=rtcmd liz
reg add %RCLICK% /ve /d \"%REMOTE% %CMD%\" /f
reg add %RCLICK% /v IconFile /d "shell32.dll" /f
reg add %RCLICK% /v IconIndex /t REG_DWORD /d 23 /f
RtCmd rclick su
```

## 7.3 Joker (Wildcard)

### 7.3.1 Objektjoker (\*)

Wird intelligent durch ein Objekt ersetzt. Sind mehrere Objekte verfügbar, so wird das neuste ausgewählt.

pb s=Briefe t=*
pb s=Briefe t=071025_194843.zip
pr s=071025_194843.zip t=*
pr s=071025_194843.zip t=C:\Users\Hans\Dokumente\Briefe
pr s=* t=Briefe
pr s=071025_194843.zip t=Briefe

### 7.3.2 Laufwerksjoker (\*FD,\*HD,\*RD,\*CD,\*NET)

<b>*FD</b>	<b>Floppydisk</b>	Diskettenlaufwerke
<b>*HD</b>	<b>Harddisk</b>	Festplatten
<b>*RD</b>	<b>Removable Disk</b>	Wechselfestplatten, USB- und Memory-Sticks
<b>*CD</b>		CD und DVD Laufwerke
<b>*NET</b>		Netzwerkordner

Laufwerksjoker werden durch alle verfügbaren Laufwerke des Typs ersetzt.

pb s=Briefe t=*HD\Januar.zip
pb s=Briefe t=c:\Januar.zip t=d:\Januar.zip
pr s=*NET\share\Januar.zip t=Briefe
pr s=\\Server1\share\Januar.zip s=\\Server2\share\Januar.zip t=Briefe

### 7.3.3 Pfadjoker (\*DOC,\*ALL,\*USR)

	Vista™	XP, Server™2003
<b>*DOC</b>	Dokumente	Eigene Dateien
<b>*ALL</b>	Öffentliche Dokumente	Dokumente
<b>*USR</b>	z.B. C:\Users	z.B. C:\Dokumente und Einstellungen

Pfadjoker werden durch die entsprechenden Ordner der aktuellen Installation ersetzt.

pb s=*DOC\Briefe
pb s=C:\vis_u\Hans\Documents\Briefe
pb s=*USR\Maria\Documents\Briefe
pb s=C:\vis_u\Maria\Documents\Briefe

### 7.3.4 Archivjoker (\*ROOT,\*ARCH)

**\*ROOT** wird intelligent durch einen Archivpfad ersetzt.

**\*ARCH** wird immer durch RtArch\\*ROOT ersetzt.

pb s=data t=M:\*ROOT\Januar.zip
---------------------------------

```
pb s=data t=M:\Hans\Documents\data\Januar.zip
```

```
ib t=C:\*ARCH\clean_and_fast.ib
```

```
ib t=C:\RtArch\_PC\Vista_32\clean_and_fast.ib
```

### 7.3.5 Filter in \*ROOT und \*ARCH

Bei Private-Restore und bei Install-Restore kann zum Archivjoker eine Filterzahl angegeben werden, um fremde Archive auszuwählen.

\*xROOT oder \*xARCH

Bei Private-Restore ist die Auflösung des Filters davon abhängig, ob der Zielordner einem bestimmten Benutzer(user) zugeordnet werden kann.

Private-Restore user	fremde Benutzer	fremde Ordner	alle
Private-Restore	fremde Rechner	fremde Ordner	alle
Install-Restore	fremde Rechner	fremde Betriebssysteme	alle
0			
1	x		
2		x	
3	x	x	
4			x

### 7.3.6 \*ROOT in RT\_LOG, RT\_ERROR, RT\_SCHEDULE

Beispiel-Tabelle für die Ersetzung von \*ROOT:

	RT_LOG
Console sichtbar	Hans\_LOG_\Console
Console unsichtbar	Hans\_LOG_\Hidden
RtCmd (-q Option)	Hans\_LOG_\RtCmd32
	RT_ERROR
Console sichtbar	Hans\_ERROR_\Console
Console unsichtbar	Hans\_ERROR_\Hidden
Fehler in c_e.exe	Hans\_ERROR_\c_e64
Fehler in RtHost.exe	Hans\_ERROR_\RtHost64
RtCmd (-q Option)	Hans\_ERROR_\RtCmd64
	RT_SCHEDULE
Console SCHEDULE Status	Hans\_SCHEDULE_

## 7.4 Worterklärungen

### 7.4.1 Active Directory

Verzeichnis-Dienst, der in allen Server-Betriebssystemen enthalten ist. Die Hauptaufgabe ist es, Benutzer-Konten auf allen Rechnern im Netzwerk bereitzustellen und zu verwalten.

Nachteilig ist der nicht unerhebliche Administrations- und Ressourcen-Aufwand.

In kleinen Netzwerken kann auf ein Active Directory verzichtet, und stattdessen ein Konfigurations-Script eingesetzt werden, um die Benutzerkonten bereitzustellen.

## 7.4.2 Anmeldedaten (Credentials)

Verschiedene Reuschtols Funktionen können unter einem fremden Benutzer-Konto und auf einem anderen Rechner (Remote-Betrieb) ausgeführt werden. Dabei wird immer das selbe Format für die Anmeldedaten verwendet:

```
\\[MACHINE] : [USER] : [PASSWORD]
```

Ist MACHINE leer, so wird der lokale Rechner ausgewählt:

```
\\:Hans:strenggeheim
```

Ist USER leer, so wird das System-Konto ausgewählt. Sind Sie Administrator, so wird für das Systemkonto kein Passwort benötigt. Wenn nicht, muss der Backup-Service installiert und der Administrator ein Backup-Passwort festgelegt haben (Console: Einstellungen->Backup-Basswort).

```
\\
```

Lokales Systemkonto.

```
\\::strenggeheim
```

Lokales System-Konto mit Backup-Passwort.

```
\\PC::strenggeheim
```

System-Konto auf PC mit Backup-Passwort.

Ist PASSWORT leer, so wird nach dem Start des Kommandos das Passwort abgefragt, sofern ein solches erforderlich ist.

## 7.4.3 Berechtigungen (Access Control List)

Auf NTFS Laufwerken wird jedem Ordner und jeder Datei eine Liste mit folgenden Informationen angehängt:

- Wer darf eine Datei lesen oder verändern (Discretionary Access Control List).
- Soll überwacht werden, wer wann eine Datei gelesen oder verändert hat (System Access Control List).

Bei Install-Backup werden die Berechtigungen immer archiviert und mit Install-Restore wieder hergestellt. Bei Private-Backup ist diese Funktion für Laufwerke ein- und für Ordner ausgeschaltet, kann aber bei Bedarf aktiviert werden.

## 7.4.4 Bootmenü

Das Windows® Bootmenü erscheint immer beim Start des Rechners und erlaubt es dem Benutzer eine beliebige Installation auszuwählen. Wenn innerhalb der Auswahlzeit (normalerweise 3 Sekunden) keine Eingabe mit den Pfeil-Auf- oder Pfeil-Ab-Tasten erfolgt, dann wird die Voreinstellung gestartet.

## 7.4.5 EFS

Encrypting File System oder Festplattenverschlüsselung. Ein in Windows® integriertes sicheres Verschlüsselungssystem für Festplatten. Private-Backup nutzt EFS für die Verschlüsselung von Archiven. EFS ist sehr zu empfehlen, da es keine Passwort-Eingabe benötigt. Leider ist EFS nicht in allen Windows®-Versionen verfügbar. Bitte informieren Sie sich vor dem Kauf des Betriebssystems.

## 7.4.6 Exit

Rückgabe-Code, jedes Programm oder Script gibt beim Beenden eine Zahl zurück. Der Programmierer kann selbst entscheiden, welche Zahl er zurückgibt. Oft wird 0 bei Erfolg und eine Zahl ungleich 0, Fehlercode, bei Misserfolg verwendet.

```
exit 99
```

Mit diesem Befehl wird ein Script beendet und die Zahl 99 zurückgegeben.

## 7.4.7 Geplante Task

Der Windows® Zeitplandienst 'Geplante Task' wird über die Systemsteuerung oder das 'schtasks' Kommando erreicht. Er bietet eine vielseitige Möglichkeit, um ein Hintergrundprogramm zu festgelegten Zeiten auszuführen. Ab Vista™ können auch Termine automatisch nachgeholt werden, die ausgefallen sind, weil der Rechner zum angegebenen Zeitpunkt ausgeschaltet war. Eine geplante Task arbeitet unabhängig davon, ob ein Benutzer angemeldet ist oder nicht. Bei der Einrichtung muss deshalb ein Benutzerkonto und das zugehörige Benutzerpasswort angegeben werden. Die Datensicherung mit einer geplanten Task ist nur dann sinnvoll, wenn mehrere Benutzer auf dieselben Daten zugreifen. Ansonsten ist die SCHEDULE Funktion von Console-Editor zu bevorzugen, die besonders in großen Netzwerken einfacher zu administrieren ist.

## 7.4.8 Hardlinks

Dateien, die nur einmal auf der Festplatte existieren, aber mehrmals an verschiedenen Orten angezeigt werden. Vista™ enthält viele Hardlinks. Die Festplatte ist dadurch weniger voll als angezeigt. Mit 'rtcmd hardrep' können Hardlinks aufgelistet werden.

## 7.4.9 Hive

Haufen, als Hive wird eine Registrierstrukturdatei bezeichnet. Diese Dateien werden benutzt, um Daten der Registrierdatenbank auf der Festplatte zu speichern.

Die Registrierdatenbank wird aus folgenden Hives aufgebaut:



- SAM
- SECURITY
- SOFTWARE
- SYSTEM
- COMPONENTS (nur Vista™)
- BCD00000000 (nur Vista™)

Um Hives zu exportieren, kann das Windows® Programm Regedit oder [Registry Export](#) benutzt werden.

#### 7.4.10 Integrationszahl

	Fehler	Warnungen	Assistent
<b>0</b>			
<b>1</b>	x		
<b>2</b>		x	
<b>3</b>	x	x	
<b>4</b>			x
<b>5</b>	x		x
<b>6</b>		x	x
<b>7</b>	x	x	x

#### 7.4.11 Netzwerkcluster

Mehrere PCs, die über ein Netzwerk miteinander verbunden sind.

Private-Backup ermöglicht die Datensicherung auf mehreren Rechnern gleichzeitig. Sind die Rechner räumlich voneinander getrennt, so kann mit vorhandenen Arbeitsstationen eine höhere Datensicherheit erreicht werden als mit den sonst üblichen speziellen Backup Servern.

#### 7.4.12 NTFS

Festplattenformat, das seit Windows® XP als Standard benutzt wird. Im Gegensatz zu FAT32(Windows® 98) unterstützt NTFS [Berechtigungen](#) und [EFS-Verschlüsselung](#).

Bei Windows® Home ist EFS abgeschaltet und kann nicht benutzt werden.

#### 7.4.13 RAW-Daten

Roh-Daten, als RAW-Daten werden hier Dateien bezeichnet, die mit EFS verschlüsselt auf einer Festplatte abgelegt wurden. Ein normaler Benutzer hat mit RAW-Daten nichts zu tun, denn für den autorisierten Benutzer werden alle Dateien automatisch entschlüsselt, sobald er sie von der Festplatte liest.

Mit speziellen Funktionen kann aber auch auf die verschlüsselten RAW-Daten zugegriffen werden. Diese Funktionen sind für Benutzer, die Dateien archivieren, diese aber nicht lesen dürfen (Backup-Administratoren).

Private-Backup erlaubt die Archivierung von RAW-Daten. Dabei ist aber Folgendes zu beachten:

- Viele Zip-Programme können Archive mit RAW-Daten nicht verarbeiten.
- RAW-Daten können nicht komprimiert werden. Dies liegt an der Sache selbst, da verschlüsselte Daten keine Informationen über die Originaldaten enthalten dürfen. Ziparchive mit RAW-Daten sind deshalb etwa doppelt so groß wie normale, verschlüsselte oder versiegelte Archive.

#### 7.4.14 Reparsepoints

Ordner oder Laufwerke, die nicht existieren. Öffnet man einen Reparsepoint, so landet man in einem anderen Ordner, der sich auch auf einem fremden Rechner befinden kann. Typische Reparsepoints sind Laufwerks-Buchstaben, die einem Ordner im Netzwerk zugeordnet sind. Vista™ enthält viele Reparsepoints. Mit 'rtcmd hardrep' werden auch diese angezeigt.

#### 7.4.15 RT\_LOG, RT\_ERROR, RT\_SCHEDULE

Umgebungsvariablen, die vor dem Start bzw. der Installation von Reushtools gesetzt werden können, um das Protokollverhalten zu steuern. Die Syntax entspricht der von [Private-Backup](#).

Voreinstellung:

```
tf30=%SystemDrive%\*ARCH\*
```

Weitere Informationen in [Absatz7.3.6](#).

### 7.4.16 Script

Ein Script ist eine Textdatei, die Kommandos und Kommentarzeilen enthält. Um ein Script auszuführen, wird ein Kommandozeileninterpreter benötigt. In Windows® ist 'cmd.exe' enthalten. Während der Standardinstallation von Reuschttools werden verschiedene Beispielscripts in den Ordner 'Start->Programme->Reuschttools->Scripts' kopiert. Um ein Script zu betrachten oder zu bearbeiten, kann 'Bearbeiten' aus dem Kontextmenü gewählt werden.

### 7.4.17 Tastenkombination (Hotkey)

Ein oft verwendetes Programm kann mit einer Tastenkombination gestartet werden. Dazu wird zuerst eine Verknüpfung angelegt und dieser anschließend die Tastenkombination zugeordnet.

Die Verknüpfung muss sich entweder auf dem Desktop oder im Startmenü befinden:

- Klick mit der rechten Maustaste auf Reuschttools->Hotkeys und Öffnen auswählen.
- Verknüpfung wie in Absatz 7.4.19 erstellen.
- Klick mit der rechten Maustaste auf die neue Verknüpfung und 'Eigenschaften' wählen, um die gewünschte Tastenkombination einzugeben.

### 7.4.18 Template

Vorlage, Private-Backup und Install-Backup benutzen Templates. Dabei wird nach früheren Zip-Dateien gesucht und diese als Vorlage verwendet.

- Es werden nur Veränderungen seit der letzten Archivierung angezeigt. Der Anwender erkennt dadurch sofort, an welchen Dateien gearbeitet, und dass diese sicher archiviert wurden.
- Die Archivierung erfolgt bis zu 40 mal schneller als mit herkömmlichen Programmen, wenn ein installiertes Programmpaket seit der letzten Installationssicherung nicht verändert wurde.
- Die Archivierung erfolgt bis zu 5 mal schneller als mit herkömmlichen Programmen, wenn sich nur eine von vielen Dateien in einem Ordner verändert hat.

### 7.4.19 Verknüpfung im Startmenü

Um ein Programm aus dem Startmenü auszuführen, kann eine Verknüpfung angelegt werden:

- Rechtsklick auf Start und Klick auf 'Öffnen' oder 'Öffnen alle Benutzer'.
- Rechtsklick in den Hintergrund des neuen Fensters und Klick auf 'Neu->Verknüpfung'.
- Im nun folgenden Assistenten-Fenster muss zuerst die Command Line (Speicherort des Elements) und dann der Name der Verknüpfung eingegeben werden.

Command Line:

```
c_e -xp rtcmd pb s=*DOC\data tf30=*HD\*ARCH\* tf5=*RD\*ARCH\*
```

Name:

Backup data

Diese Verknüpfung sichert den eigenen Ordner 'data' auf der Festplatte und einem USB-Stick.

### 7.4.20 Versiegelung

Wenn ein Archiv nur mit EFS verschlüsselt ist, kann es:

- Versehentlich beim Kopieren auf andere Datenträger entschlüsselt werden.
- Nur auf lokalen Datenträgern, die NTFS benutzen, verschlüsselt gespeichert werden.

Um eine verschlüsselte Datensicherung auf allen Datenträgern und Netzwerken zu ermöglichen, werden Zip Archive bei Bedarf automatisch versiegelt.

Bei der Versiegelung wird ein Archiv zuerst mit EFS verschlüsselt. Danach werden die verschlüsselten Daten von der Festplatte im Raw Modus gelesen und in eine unverschlüsselte Datei mit der Endung .seal geschrieben.

Interessierte Kunden können auf Anfrage den Quelltext für die Versiegelung und Entsigelung von Archiven erhalten.

### 7.4.21 VSS

Volume Shadow Copy Service oder Schattenkopierer.

Ein Programm, das im Windows® Betriebssystem enthalten ist. Es ermöglicht die Archivierung von Dateien, während diese gerade benutzt werden. VSS ermöglicht z.B. ein Private-Backup von laufenden Datenbanken. Install-Backup nutzt VSS vorwiegend für die Archivierung der Registry.

VSS setzt sich aus vielen einzelnen Komponenten verschiedener Hersteller zusammen. Ein Versagen von VSS führt auch zum Versagen von Install-Backup bzw. Private-Backup.

### 7.4.22 Windows® PE

Preinstallation Environment oder Vorinstallationsumgebung.

Ist ein startfähiges Windows® das normalerweise direkt von einer CD oder DVD gestartet wird. Windows® PE besitzt eingeschränkte Funktionalität, die aber ausreicht um eine komplette Windows-Installation mit Install-Restore entweder von einer DVD, der Festplatte oder dem Netzwerk wiederherzustellen.

Windows® PE kann mit folgenden DVDs direkt gestartet werden:

1. Windows®-Installations-DVD.
2. 'OEM Preinstallation Kit' DVD, wird mit den Windows® 7 OEM-Versionen geliefert.
3. Systemreparaturdatenträger. Wenn Ihr Computer ohne Windows®-Installations-DVD ausgeliefert wurde, empfiehlt sich die Herstellung einer Start-DVD. Bei Windows® 7 wird dazu.

```
Systemsteuerung->System und Sicherheit->Sicherung des Computers..
```

aufgerufen. Auf dieser Seite wählen Sie 'Systemreparaturdatenträger erstellen'.

4. Install-Restore Recovery-DVD. Wird vom Computerhersteller zusammen mit einem Windows® Rechner ausgeliefert. Diese enthält sowohl Windows® PE als auch einen Install-Backup Datensatz. Der Install-Restore Assistent startet automatisch um die original Windows-Installation wiederherzustellen, ohne dass dabei persönlich Dateien gelöscht werden.

Um Windows® PE von einer DVD zu starten muss das entsprechende DVD Laufwerk im BIOS als Startlaufwerk markiert sein. Bei neuen Rechnern ist dies oft die Voreinstellung.

### 7.4.23 Ziffern-Archiv

Ein Ziffern-Archiv, ist ein Archiv dessen Name mit einer Ziffer beginnt.

```
071025_194843.zip
```

Ziffern-Archive werden von Private-Backup und Install-Backup mit der TCONTROL f-Option verwaltet. Wird ein Ziffern-Archiv z.B. in

```
Januar.zip
```

umbenannt, kann es nicht mehr mit der f-Option gelöscht werden.

### 7.4.24 Zip-Datei

Reißverschlussdatei, in einer Zip-Datei werden mehrere Dateien in nur einer Datei komprimiert gespeichert.

Stellen Sie sich eine Sporttasche vor, in die mehrere Kleidungsstücke hineingepresst wurden und die anschließend mit dem Reißverschluss verschlossen wurde. Die Handhabung der Sporttasche ist wesentlich einfacher als die der einzelnen Kleidungsstücke.

Alle modernen Windows® Betriebssysteme können Zip-Dateien ohne Zusatzsoftware verarbeiten. Das Format wurde von Phil Katz entwickelt und der Öffentlichkeit kostenlos zur Verfügung gestellt. Danke!

### 7.4.25 Zip-Verschlüsselung

Private- und Install-Backup benutzen die original Zip-Verschlüsselung. Dadurch können verschlüsselte Ziparchive von fast allen Zip-Programmen entschlüsselt werden, sofern man das Passwort kennt. Diese Verschlüsselung wird auch von modernen Windows® Systemen unterstützt.

Die Zip-Verschlüsselung wurde 1989 veröffentlicht und seither wiederholt kritisiert:

- A Known Plaintext Attack on the PKZIP Stream Cipher, Eli Biham und Paul C. Kocher
- ZIP Attacks with Reduced Known Plaintext, Michael Stay

In vielen Zip-Programmen wurde die Verschlüsselung schlecht programmiert. Das hat auch historische Gründe, denn der Export von starken, tatsächlich funktionierenden Verschlüsselungen aus den USA war lange Zeit verboten.

Private- und Install-Backup benutzen im Gegensatz zu herkömmlichen Zip-Programmen zusätzliche Sicherheitsmechanismen:

- Statt Pseudo-Zufallszahlen werden tatsächliche Zufallszahlen eingesetzt.
- Bei aktivierter Zip-Verschlüsselung werden die Codetabellen (Huffman Codes) verwürfelt, wodurch die oben genannte 'Plaintext Attack' verhindert wird.

Es gibt inzwischen verschiedene kommerzielle Programme, um verschlüsselte Ziparchive zu knacken (z.B. Advanced ZIP Password Recovery, [www.elcomsoft.com](http://www.elcomsoft.com)). Diese Programme zeigen, dass die von Private-Backup benutzte Verschlüsselung sicher ist, sofern ein sicheres Passwort verwendet wird.

## 7.5 Wichtige Information

### 7.5.1 Credits

- Info-ZIP
- NSIS
- NSIS Modern User Interface 2
- Code-Projekt
- Sys-Internals
- Boost
- Python

- SCons
- Halibut

## 7.5.2 Markennamen

Der Inhalt der mitgelieferten Software sowie dieses Handbuchs kann ohne Ankündigung geändert werden. Alle Markennamen und Marken sind Eigentum der jeweiligen Inhaber. Alle Marken dienen lediglich der Information.

# Inhaltsverzeichnis

1: Install-Backup.....	2	6.2.5 decrypt, entschlüsselt ein Objekt.....	21
1.1 Tutorial (online).....	2	6.2.6 delfile, löscht eine Datei.....	21
1.2 Frequently Asked Questions (Online).....	2	6.2.7 deltree, löscht einen Ordner.....	21
1.3 Command Line.....	2	6.2.8 encrypt, verschlüsselt ein Objekt.....	21
1.3.1 CONTROL.....	2	6.2.9 list, zeigt den Inhalt eines Ordners oder Laufwerks.....	21
1.3.2 PASSWORD.....	2	6.2.10 seal, speichert eine Datei im RAW-Format.....	22
1.3.3 TCONTROL.....	2	6.2.11 sopen, öffnet ein RAW-Archiv (.seal).....	22
1.3.4 TARGET.....	2	6.2.12 unseal, konvertiert eine Datei vom RAW-Format.....	22
2: Install-Restore.....	4	6.3 Windows® Registry.....	22
2.1 Tutorial (online).....	4	6.3.1 delkey, löscht einen Registry-Schlüssel.....	22
2.2 Frequently Asked Questions (Online).....	4	6.3.2 hc, vergleicht zwei Hives.....	22
2.3 Command Line.....	4	6.3.3 hs, zeigt einen Hive.....	22
2.3.1 CONTROL.....	4	6.3.4 ii, zeigt die Windows® Ordner.....	22
2.3.2 SOURCE.....	5	6.3.5 rc, vergleicht die Registry.....	22
2.3.3 TARGET.....	5	6.3.6 re, exportiert die Registry.....	22
3: Private-Backup.....	6	6.3.7 rs, zeigt die Registry.....	23
3.1 Tutorial (online).....	6	6.4 Automatisierung.....	23
3.2 Frequently Asked Questions (Online).....	6	6.4.1 icons, zeigt alle Icons aus c_e.exe und shell32.exe.....	23
3.3 Command Line.....	6	6.4.2 mb_ok, Fenster mit OK.....	23
3.3.1 CONTROL.....	6	6.4.3 mb_yes, Fenster mit Ja.....	23
3.3.2 PASSWORD.....	7	6.4.4 mb_yesno, Fenster mit Ja-Nein.....	23
3.3.3 SOURCE.....	7	6.4.5 sleep, wartet.....	23
3.3.4 TCONTROL.....	7	6.4.6 start, startet einen Dienst.....	23
3.3.5 TARGET.....	7	6.4.7 stop, beendet einen Dienst.....	23
4: Private-Restore.....	9	6.4.8 wc, schließt ein Fenster.....	24
4.1 Tutorial (online).....	9	6.4.9 zoom, verändert die Bildschirm-Auflösung.....	24
4.2 Frequently Asked Questions (Online).....	9	6.5 Reushtools Setup.....	24
4.3 Command Line.....	9	6.5.1 backuppwd, setzt ein Backup-Passwort.....	24
4.3.1 CONTROL.....	9	6.5.2 liz, zeigt die Reushtools-Lizenz.....	24
4.3.2 PASSWORD.....	9	6.5.3 noblub, deaktiviert eine Warn-Meldung.....	24
4.3.3 SOURCE.....	10	6.5.4 path, erweitert die PATH Variable.....	24
4.3.4 TARGET.....	10	6.5.5 rclick, registriert Einträge im Kontext-Menü.....	24
5: Console-Editor.....	11	6.5.6 root, zeigt den Reushtools Installations-Pfad.....	25
5.1 Handling.....	11	6.5.7 setup, registriert Reushtools.....	25
5.1.1 Protokoll.....	11	7: Appendix.....	26
5.1.2 Windows® PowerShell™.....	11	7.1 Reushtools Konfiguration.....	26
5.1.3 Cygwin Bash Shell.....	11	7.1.1 persönliche und systemübergreifende Installationen.....	26
5.1.4 Input-Scripts.....	11	7.1.2 Konfiguration mit den Setup-Assistenten.....	26
5.1.5 Scripts beim Abmelden oder Herunterfahren.....	12	7.1.3 Bereitstellung ohne Installationsprogramm.....	26
5.1.6 Scripts mit Gruppenrichtlinien starten.....	12	7.1.4 Lautlose Installation.....	26
5.1.7 Tipps mit Scripts.....	12	7.1.5 Upgrade.....	28
5.2 Command Line.....	13	7.2 Einträge im Kontextmenü.....	28
5.2.1 CONTROL.....	13	7.2.1 RClick.dll.....	28
5.2.2 CREDENTIALS.....	14	7.2.2 Iconklassen.....	28
5.2.3 [D,T]SCHEDULE.....	14	7.2.3 Registrierung.....	28
5.2.4 PATH.....	15	7.2.4 Beispiele.....	29
5.2.5 FILE.....	15	7.3 Joker (Wildcard).....	30
5.2.6 PARAMETER.....	15	7.3.1 Objektjoker (*).....	30
6: Tools.....	17	7.3.2 Laufwerksjoker (*FD,*HD,*RD,*CD,*NET).....	30
6.1 Benutzer-Konten.....	17	7.3.3 Pfadjoker (*DOC,*ALL,*USR).....	30
6.1.1 account, erstellt Benutzer-Konten.....	17	7.3.4 Archivjoker (*ROOT,*ARCH).....	30
6.1.2 Backup-Service, Dienst für eingeschränkte Benutzer-Konten.....	17	7.3.5 Filter in *ROOT und *ARCH.....	31
6.1.3 efskey, generiert Schlüssel für das Datei-System.....	17		
6.1.4 password, generiert Passworte.....	18		
6.1.5 profiler, verschiebt Ordner für regelmäßige Backups.....	18		
6.1.6 Zeitsparkasse, Hilfsprogramm gegen PC-Abusus.....	20		
6.2 Datei-System.....	21		
6.2.1 access, setzt Berechtigungen.....	21		
6.2.2 acl, zeigt Berechtigungen.....	21		
6.2.3 tree, shows a file tree.....	21		
6.2.4 cleantree, erstellt einen leeren Ordner.....	21		

7.3.6 *ROOT in RT_LOG, RT_ERROR, RT_SCHEDULE.....	31	7.4.14 Reparsepoints.....	33
7.4 Worterklärungen.....	31	7.4.15 RT_LOG, RT_ERROR, RT_SCHEDULE.	33
7.4.1 Active Directory.....	31	7.4.16 Script.....	34
7.4.2 Anmeldedaten (Credentials).....	32	7.4.17 Tastenkombination (Hotkey).....	34
7.4.3 Berechtigungen (Access Control List)..	32	7.4.18 Template.....	34
7.4.4 Bootmenü.....	32	7.4.19 Verknüpfung im Startmenü.....	34
7.4.5 EFS.....	32	7.4.20 Versiegelung.....	34
7.4.6 Exit.....	32	7.4.21 VSS.....	34
7.4.7 Geplante Task.....	32	7.4.22 Windows® PE.....	34
7.4.8 Hardlinks.....	32	7.4.23 Ziffern-Archiv.....	35
7.4.9 Hive.....	32	7.4.24 Zip-Datei.....	35
7.4.10 Integrationszahl.....	33	7.4.25 Zip-Verschlüsselung.....	35
7.4.11 Netzwerkcluster.....	33	7.5 Wichtige Information.....	35
7.4.12 NTFS.....	33	7.5.1 Credits.....	35
7.4.13 RAW-Daten.....	33	7.5.2 Markennamen.....	36