Backup Konzept

Autor: Florian Bauer, gehtnicht.at

Version: 1.2

Letzte Änderung: 30.05.2013

Inhalt

Einleitung

Dieses Backup Konzept wird erarbeitet, weil durch einige Ausfälle von Hardware oder ähnlicher Umstände große Datenmengen verloren gingen. Vor allem geht bei Datenverlust viel Zeit verloren, um den zuvor gewohnten Zustand wiederherzustellen.

Arten von Backups

Es gibt im Zusammenhang mit diesem Konzept Datei-Backups und Laufwerk-Backups:

- Beim **Datei-Backup** werden ausgewählte Dateien und Ordner gesichert (z.B.: Eigene Dokumente, Eigene Musik, Eigene Videos).
- Beim **Laufwerk-Backup** wird die „gesamte Platte“ gesichert (z.B. „C:“).

Exkurs Volume Shadow Service: Dank Volume Shadow Service (VSS) ist es mit beiden Arten von Backups möglich, Backups zu machen, während der Computer verwendet wird. Das Volume Shadow Service erstellt einen „Schatten“ des Laufwerks zu Beginn des Backup-Vorgangs. Dieser Schatten wird gesichert. Sämtliche Änderungen nach Erstellung des Schattens sind im Backup nicht enthalten. Sie werden erst beim nächsten Backup gesichert.

Stellt man die beiden Backup-Arten gegenüber ist das **Laufwerk-Backup attraktiver**, weil es kompletter ist und kaum ein Laufwerk-Backup kann nicht geöffnet werden, um einzelne Dateien zu extrahieren. Beim Laufwerk-Backup kann jedoch keine Datei vergessen oder übersehen werden. Bei der Wiederherstellung eines Systems ist man mit einem Laufwerk-Backup ebenfalls besser bedient.

Die „Komplettheit“ des Laufwerk-Backups geht entsprechend zu Lasten der Zeit, die zum Erstellen eines Backups benötigt wird, und zu Lasten des Platzes, der für das erstellte Backup benötigt wird.

Evaluierte Software

Während der Erstellung des Konzepts wurde folgende Software zum Erstellen von Backups evaluiert, deren Ergebnis in den folgenden Kapiteln kurz beschrieben wird.

Die evaluierte Software ist durchgehend für den Heimgebrauch frei einzusetzen.

Microsoft SyncToy 2.1

Das Tool ist schnell eingerichtet und es kann per Command-Line gestartet werden.

Wird nicht eingesetzt, weil Laufwerk-Backups die bevorzugte Strategie sind.

Robocopy

Das Tool hat kein GUI. Es kann per Command-Line gestartet werden und unterstützt Konfigurationsfiles. Lt. diversen Forumseinträgen ist es zuverlässiger als SyncToy.

Wird nicht eingesetzt, weil Laufwerk-Backups die bevorzugte Strategie sind.

DriveImage XML v2.44

Das Tool sichert (relativ langsam) ganze Festplatten und Sticks. Leider war das Backup vom Teststick korrupt. Die wiederhergestellten Dateien waren zwar gleich groß, hatten aber nicht mehr dieselben Checksummen.

Wird nicht eingesetzt, weil das Backup mehrfach korrupt war *(eventuell wegen kaputter Abhängigkeit, wie bei AOMEI Backupper)*.

AOMEI Backupper v1.1

Das Tool funktioniert auf dem Testrechner überhaupt nicht. Sobald ein Backup (16GB FAT USB-Stick) gestartet wird, erhält man eine wenig hilfreiche Fehlermeldung, dass ein Treiber nicht in Ordnung sei. Schade, da die Feature-Liste sehr vielversprechend schien.

Wird nicht eingesetzt, da damit kein Backup erstellt werden konnte.

EaseUS Todo Backup Free v5.8

Das Tool kann grundsätzlich alles, was für ein Laufwerk-Backup benötigt wird, jedoch kann es nicht von der Command-Line gestartet werden, was eine Automatisierung verhindert.

Wird nicht eingesetzt, da das Backup nicht per Command-Line gestartet werden kann.

Macrium Reflect Free v5.1

Das Tool kann grundsätzlich alles, was für ein Laufwerk-Backup benötigt wird. Es kann keine Sticks sichern und auch Datei-Sicherungen werden nur in der käuflichen Version angeboten. Die Backups werden schnell erstellt, die Checksummen stimmen überein.

Wird eingesetzt.

BackUp Maker v6.504

Das Tool wurde als Ergänzung zu Macrium Reflect Free v5.1 evaluiert. Für den NAS wird die Datei-Backup Art benötigt. Das Tool zippt die Backups, es kann inkrementelle Backups und prüft die Integrität. Die Command-Line kann leider nur mäßig befriedigend eingesetzt werden, weshalb das Tool ausscheidet.

Wird nicht eingesetzt, da das Backup per Command-Line unkorrekte und vorschnelle Rückgabe an den Aufrufer verursacht.

Areca Backup v7.3.3

Das Tool wurde als Ergänzung zu Macrium Reflect Free v5.1 evaluiert. Für den NAS wird die Datei-Backup Art benötigt. Das Tool zippt die Backups, es kann inkrementelle Backups und prüft die Integrität.

Wird eingesetzt *(für die Sicherung des NAS')***.**

Backup-Vorgang

Überblick

Das Backup soll so einfach wie möglich über die Bühne gehen: Anstecken, Sicherung erstellen, Abstecken.

Damit die Sicherheit nicht zu kurz kommt, wird das Backup pro Rechner in einem Truecrypt Container gespeichert. Jeder kennt nur die Passphrase seines Backup-Containers auf der Backup-Platte. So ist auch eine Backup-Platten-Rotation möglich und im Falle eines Diebstahls sind die Daten des Backups ohne die Passphrase wertlos.

Zwecks Sicherheit ist der Vorgang etwas komplexer geworden: Anstecken, *Truecrypt Container mounten*, Sicherung erstellen, *Truecrypt Container unmounten*, Abstecken.

Software-Unterstützung durch Backstage

Damit dieser Vorgang für den wöchentlichen Gebrauch so einfach wie möglich bleibt, wird das Programm **Backstage** von *gehtnicht.at* entwickelt. Es wird mit einem gewünschten Profil (das auf der Backup-Platte hinterlegt wird) gestartet. Im Profil ist hinterlegt, welcher Truecrypt Container gemountet wird und welche Sicherung im Anschluss gestartet wird. Nachdem die Sicherung abgeschlossen ist, wird der Truecrypt Container ungemountet und die Backup-Platte kann ausgeworfen werden.

Wiederherstellungs-Vorgang

Der Wiederherstellungs-Vorgang wird mittels des gewählten Backup-Tools durchgeführt. Einmalig wird geprüft, ob das Backup korrekt auf eine andere Festplatte wiederhergestellt werden kann und anschließend das Betriebssystem korrekt weiterläuft und alle Dateien in Ordnung sind.

Mittels Macrium Reflects *Rescue Media Wizard* wird ein *Windows PE* Image erstellt. Mit diesem Image können Backups wiederhergestellt werden.

Dieses Rescue Media kann auf einem anderen Rechner erstellt werden, als auf dem Beschädigten.

Für das Backup wurde ein WinPE custom Image erstellt (Backstage.wim). Es handelt sich dabei um ein Standard WinPE 3.0 Image mit folgenden vorinstallierten Programmen: Notepad++ v6.0, 7-Zip v9.20, TrueCrypt v7.1a, Disk Wipe v1.7. Außerdem wurde der „ScratchSpace“ auf 512MB gesetzt.

Backup Setup

Damit Backups transparent erstellt werden können, muss die Software aus Kapitel Benötigte Software auf dem Rechner installiert sein.

Anschließend müssen die in Kapitel Einmalige Vorbereitungen beschriebenen Schritte durchgeführt werden.

Nun kann das Backup mit Backstage durchgeführt werden, so einfach wie es in Backup-Vorgang/Überblick beschrieben wurde!

Benötigte Software

TrueCrypt v7.1a

Version 7.1a vom 07.02.2012, http://www.truecrypt.org/downloads

Dieses Tool stellt die Verschlüsselung der Backups bereit. Wer auf die Verschlüsselung des Backups verzichten will, benötigt das Tool nicht.

Hinweis: Nach der Installation kann das Tray-Icon entfernt werden!

Macrium Reflect Free v5.1

Version 5.1.5870 vom 17.04.2013, http://www.macrium.com/reflectfree.aspx

Dieses Tool erstellt die tatsächlichen Backup-Files von Laufwerken.

Hinweis: In den Defaults bei Advanced die 20 Sekunden Vorlaufzeit abschalten!

Areca Backup v7.3.3 [Optional]

Version 7.3.3 vom 12.05.2013, http://www.areca-backup.org/

Dieses Tool wird für das Datei-Backup von NAS oder anderen Netzlaufwerken benötigt. Wer keinen NAS daheim hat, benötigt das Tool nicht.

Backstage

Dieses Tool ist zum Zeitpunkt des Erstellens des Dokuments noch nicht released.

Einmalige Vorbereitungen

TrueCrypt Container erstellen

1. TrueCrypt starten
2. Menü *Volumes*, *Create New Volume...*
3. Option *Create an encrypted file container* auswählen und auf *Next* klicken
4. Option *Standard TrueCrypt volume* auswählen und auf *Next* klicken
5. In Feld *Volume Location* einen Dateinamen wählen und auf *Next* klicken
   Hinweis: die Datei wird am besten bereits auf der Backup-Platte erstellt
6. In Feld *Encryption Algorithm* den Wert *AES* ausgewählt lassen, auch Feld *Hash Algorithm* auf Wert *RIPEMD-160* lassen und auf *Next* klicken
7. Bei *Volume Size* die gewünschte Größe der Platte einstellen und auf *Next* klicken
   Hinweis: Es empfiehlt sich, zumindest die Größe des belegten Speichers auf der Festplatte zu nehmen, oder sogar die Größe der Festplatte. Sollte der Container zu klein werden, muss einfach vor dem nächsten Backup ein neuer Container eingerichtet werden!
   Beispiel: Für eine 232GB Platte, die bis auf 3GB voll ist, wird für das Full Backup ein Platz von 160GB benötigt.
8. Bei *Volume Password* das gewünschte Passwort eintragen und auf Next klicken
   ACHTUNG: Geht das Passwort verloren, gehen die Daten verloren, weil sie ohne das Passwort nicht mehr entschlüsselt werden können!
   Hinweis: Es empfiehlt sich, ein starkes und sicheres Passwort zu verwenden. Mit diesem Passwort wird der TrueCrypt Container verschlüsselt. Nur mit diesem Passwort kann der Inhalt des TrueCrypt Containers wieder entschlüsselt werden.
   Tipps zum Erstellen eines sicheren Passworts *lt. TrueCrypt (analog zum Hinweis im Wizard): Kein einzelnes Wort verwenden, das in einem Wörterbuch gefunden werden kann (oder eine Kombination von 2, 3 oder 4 solcher Wörter). Keine Namen oder Geburtsdaten verwenden. Das Passwort sollte nicht leicht zu erraten sein. Ein gutes Passwort ist eine Zufallskombination von großen und kleinen Buchstaben, Ziffern und Sonderzeichen, wie zum Beispiel @ ^ = $ * + etc. Empfohlen wird, dass das gewählte Passwort mehr als 20 Stellen haben soll (je länger, desto besser). Die Maximale Länge des Passworts beträgt 64 Stellen.*
9. Bei *Large Files* die Option *Yes* auswählen und auf *Next* klicken
10. Bei *Volume Format* die Option *Filesystem* auf *NTFS* lassen, *Cluster* bleibt *Default*. Das Häkchen bei *Random Pool* bleibt *angehakt*.
    Hinweis: In diesem Fenster soll ein wenig die Maus irgendwie bewegt werden, um ein wenig mehr Zufall in die Verschlüsselung hineinzubringen. Viel Spaß! ;-)

Auf *Format* klicken
Hinweis: Jetzt wird der verschlüsselte und bereits formatierte TrueCrypt Container erstellt. ***Das kann mitunter einige Stunden dauern***

11. Messagebox mit *OK* bestätigen („TrueCrypt volume has successfully been created“)
12. Bei *Volume Created* auf *Exit* klicken

Macrium Reflect XML-Backup-Profile einrichten

1. Macrium Reflect starten
2. Menü *Backup*, *Image Local Drives...*
3. Bei *Source* die Disk(s) anhaken, für die ein Backup erstellt werden soll
4. Bei *Destination* die Option *Folder* wählen und als Ordner die gemountete TrueCrypt Volume ohne Unterordner auswählen: „T:\“
   Das Häkchen bei *Use the Image ID as the file name* das Häkchen entfernen und in Feld *Backup filename* den Namen entsprechend des Hinweises eingeben und anschließend markieren und kopieren (STRG+C):
   Hinweis: Der Name setzt sich aus folgenden Teilen zusammen: Adresse (3 stellig), Bezirk (2 stellig), Name des Besitzers, Betriebssystem („Win7“ oder „WinXP“), Plattenformat (sollte im Standardfall immer „NTFS“ sein), Plattengröße in GB
   Beispiele: „Pra21 Florian Win7 NTFS 250GB“, „Lae12 Hans WinXP NTFS 200GB“, „Tue11 Sebastian Win7 NTFS 1TB“
   Wenn nicht das System gesichert wird, kann die Wahl des Namens entsprechend anders ausfallen, z.B.: „Pra21 WD Passport White FAT 100GB, NTFS 200GB“
   Auf *Next* klicken
5. Bei *Image Summary* auf *Finish* klicken
6. Im Fenster *What do you want to do now* das Häkchen bei *Run this backup now* entfernen, das Häkchen bei *Save this backup as an XML Backup Definition File* angehakt lassen
   Im Feld *Enter a name for this backup definition* den gleichen Namen, wie für *Backup filename* aus Schritt 4 verwenden. Wenn der Name kopiert wurde, kann er jetzt mit STRG+V wieder eingefügt werden
   Auf *OK* klicken
7. Die XML-Datei wurde in den *Eigenen Dateien* im Unterordner *Reflect* angelegt

Areca Backup-Profil einrichten

Wird nicht dokumentiert, da es nicht allgemein verwendet wird.

Backstage Profil einrichten

1. Basierend auf dem *SampleBackupSetting.backstage* Profil Anpassungen vornehmen.

Anhang

Quellen

Während der Ausarbeitung dieses Konzepts wurden folgende Beiträge gelesen und für eigene Zwecke weiterverwendet.

Blogeinträge mit Übersicht über Backup-Tools

http://www.techrepublic.com/blog/five-apps/five-free-and-reliable-cloning-tools/1507

http://dottech.org/95071/windows-best-free-file-drive-system-image-sector-backup-programs-review/

http://dottech.org/11628/paragon-backup-restore-free-vs-macrium-reflect-free-vs-easeus-todo-backup-vs-driveimage-xml-vs-acronis-true-image-home-which-one-should-you-use/

Macrium Reflect Free v5.1 Download

v5.1.5870 vom 17.04.2013, http://www.macrium.com/reflectfree.aspx

Areca Backup v7.3.3

v7.3.3 vom 12.05.2013, http://www.areca-backup.org/