Security & Firewalls: Backup-Lösung mit Duplicity / Ftplicity

Backup-Lösungen gibt es viele. Aber nur wenige beachten die Sicherheit und inkrementelles Backup zu gleich.
Duplicity basiert gerade auf diesen Grundlagen: Verschlüsselung, inkrementell, kleine Dateien.

Christiane Rütten Heise-Autor hat dann ein kleines Script namens `ftplicity` entwickelt, mit dem sich `duplicity` steuern läßt, und die erzeugten Dateien schnell auf einen FTP-Server als Backup hinterlegen lassen.

Installation

Von den Distributions-Paketen braucht man grundsätzlich mal Python und für das Syncronisieren die `librsync`.
Beide sind mit den jeweiligen Paketmanagern zu installieren.

Dublicity (vorher auf aktuellere Version prüfen):

```
wget http://savannah.nongnu.org/download/duplicity/duplicity-0.4.2.tar.gz
tar duplicity-0.4.2.tar.gz
tar -xvzf duplicity-0.4.2.tar.gz
cd duplicity-0.4.2/
python setup.py install
```

Ftplicity:

```
wget ftp://ftp.heise.de/pub/ct/listings/0613-216.tar.gz
tar -xvzf 0613-216.tar.gz
cd ftplicity-1.1.1/
cp ftplicity /usr/local/bin
```

Für die Verschlüsselung benötigt es noch einen GPG-Key.

Hiervon merken wir uns die achtstellige Key-ID und das Kennwort.

```
gpg –gen-key
```

Konfiguration

Mit einem ersten Aufruf von `ftplicity backup` wird unter `/root/.ftplicity/` eine Konfiguration erstellt.

In `/root/.ftplicity/conf` werden die Daten vom GPG-Key eingetragen: `GPG_KEY` und `GPG_PW`.

Die Daten des Backup-Servers kommen in die Variablen `ZIEL` und `ZIEL_PW`

Cronjobs

```
#jede Nacht ein inkrementelles Backup
00 2 * * * root /usr/local/bin/ftplicity backup
#einmal im Monat ein Full-Backup
00 4 1 * * root /usr/local/bin/ftplicity full && /usr/local/bin/ftplicity purge –force
```

Bedienung:

Die Bedienung ist relativ simpel:

```
#Inkrementelles Backup:
ftplicity backup

#Voll-Backup:
ftplicity full

#unvollständige Backups:
ftplicity clean

#unvollständige Backups aufräumen:
ftplicity clean --force

#veraltete Backups:
ftplicity purge

#veraltete Backups löschen:
ftplicity purge --force

#Backup wieder einspielen:
#source = Datei oder Verzeichnis, welches wieder hergestellt werden soll
#target = Datei oder Verzeichnis, wohin source wieder hergestellt werden soll
#from   = Alter des Backups
ftplicity fetch source target from
#Beispiel (web11 ins Orginalverzeichnis mit einem Backup von vor 4 Tagen):
ftplicity fetch /var/www/web11/ /var/www/web11/ 4d
```

Security & Firewalls: Backup-Lösung mit Duplicity / Ftplicity

Backup-Strategie:

Auf Servern sollte man niemals ein Full-Backup der Root-Partition machen. Denn im Falle eines Falles, hat man im Backup bereits den selben Fehler drin stehen, warum er momentan nicht durchstarten will.

Wenn man andererseits seinen Server neu aufsetzten läßt, sollte man dann auch nicht das alte(/veraltete) System drüber bügeln.

In ein Backup gehören die Web-Verzeichnisse, MySQL-Daten und Mailboxen. Evtl. noch die User-Verwaltung, falls sie von der installierten ISP-Software nicht automatisch neu angelegt werden würde.

Weitere Links:

- Artikel von Heise-Security: Hinter Schloss und Siegel
- Script bei Heise-Security: Ftplicity

Eindeutige ID: #1327
huschi
2008-08-05 10:45