Truecrypt : Sauver ses miches en cas de défaut du volume

Procédure

- Explications

Suite au chiffrement (forcé) du SSD qui me sert pour héberger l'OS de mon ordinateur portable sous Windoze par l'IT, j'ai eu la confirmation que quasiment rien n'est prévu pour restaurer la partition principale en cas de crash du système de fichiers. Avec le logiciel truecrypt employé, le chargeur ainsi que le tout début de la partition sont modifiés et contiennent le jeu de clefs pour pouvoir amorcer l'OS. Pour éviter une cruelle déconvenue lors d'une tentative de restauration du système de fichiers en cas de corruption du MBR ou du chargeur, il convient de procéder à une sauvegarde du jeu de clef, du chargeur de démarrage et du MBR.

- Création de l'ISO

Lancez le logiciel truecrypt, sélectionnez votre volume, cliquez sur *system*, puis sur *create rescue disk* et sauvegardez l'ISO obtenue. Veuillez noter que cette ISO n'est pas amorçable depuis une clef USB, la suite permettra de pallier à ce défaut.

- Création d'une clef USB amorçable avec les données

Sous votre OS GNU/Linux préféré, exécutez ces commandes après insertion et montage d'une clef USB formatée en FAT32.

grub:

```
sudo grub-install /dev/sdX --root-directory=/point/montage/clef
```

où X est la lettre du bloc device de votre clef USB.

on utilise memdisk pour démarrer:

```
cp /usr/lib/syslinux/memdisk /point/montage/clef/boot/
nano /point/montage/clef/boot/grub.cfg
```

avec ceci :

```
     menuentry "Truecrypt Rescue" {
            drivemap -s (hd0) (hd1)
            #L'ISO ne fonctionne pas si le disque dur ou SSD est vu en tant
que 2e disque
            linux16  /boot/memdisk iso
            initrd16 /boot/TCRD.iso
            #TCRD.iso est le nom de l'ISO qui contient vos données, à
adapter au cas par cas
     }
```

- Utilisation

Branchez la clef et vous devriez voir l'amorce de grub s'afficher, appuyez sur entrée et vous pourrez restaurer en appuyant sur F8:

- le chargeur de démarrage de truecrypt
- les entêtes (avec les clefs)
- le winloader
- ou même tout déchiffré

Vous devez absolument connaître le mot de passe utilisé pour lire les clefs.

Sources

1. http://codyps.com/2012/01/26/TCRD.html

From:
http://wiki.mirtouf.fr/ - **Da mirtouf wiki**

Permanent link:
http://wiki.mirtouf.fr/doku.php?id=truecrypt

Last update: **2015/08/14 12:11**