Coffre forts de mot de passe
Recommandations SSI
Avril 2018
Rédacteur : Eric CASSETTE
Version : 20180416

Remarque : Du point de vue de la SSI, le point le plus « respectable » du texte ci-dessous est la partie 2 (précautions à prendre).

1) Produit recommandé :

Keepass (libre, open source, totalement gratuit, certifié ANSSI-CSPN en 2010 pour sa version 1.2 Portable, nouvelles version non certifiées ANSSI, mais utilisables, bien évidemment)

2) Précautions à prendre :

Définir des mots de passe maitres très complexes (mots de passe de déverrouillage des bases de mots de passe), et assurer la confidentialité de ces mots de passe maitres.

Assurer la confidentialité des bases de mots de passe (même si théoriquement ces bases pourraient être en accès public, il n'est pas nécessaire de tenter le diable…).

Prévoir une sauvegarde des bases de mot de passe ; assurer le même niveau de confidentialité aux sauvegardes qu'aux données primaires.

Garantir l'unicité de chaque base de mots de passe (pour sa confidentialité et son intégrité) : interdire formellement les copies ou les impressions « de confort ».

Mettre en œuvre un mécanisme permettant à chacun d'avoir accès uniquement aux mots de passe nécessaires à son activité (besoin d'en connaître), en maintenant plusieurs bases de mots de passe ou en utilisant un mécanisme d'arborescence de mots de passe, si disponible.

*Prévoir la situation où on a besoin d'un mot de passe alors que l'accès en ligne aux bases de mots de passe est impossible (par exemple, en cas de coupure de courant).

Si existence d'une version imprimée, détruire de façon sûre les impressions obsolètes.

Eviter les mécanismes de protection très complexes, risquant de réduire le niveau de disponibilité (le mieux est l'ennemi du bien).

Ne pas ouvrir une base de mots de passe plus souvent que nécessaire : faire l'effort de mémoriser la dizaine de mots de passe nécessaire à son activité ordinaire...

Ne pas ouvrir une base de mots de passe plus longtemps que nécessaire (risque de vol en mémoire, de capture d'écran, etc.).

Faire attention aux mises à jour concurrentes des bases de mots de passe : définir de préférences peu d'écrivains.

Continuer à gérer les mots de passe « en bon père de famille » : l'utilisation de coffre-forts de mots de passe ne dispense de respecter la politique de gestion des mots de passe (renouvellement, complexité, changement en cas de mutation ou départ d'un personnel), y compris, et surtout, pour les mots de passe de déverrouillage...

3) Concrètement, comment stocker les bases de mots de passe ? :

Si les précautions définies ci-dessus sont respectées, on peut stocker les bases de mots de passe sur des partages réseaux dont les droits d'accès auront été correctement définis (groupes selon le « besoin d'en connaître »).