Protéger secrets et documents sensibles, même sans moyens gouvernementaux

Octobre 2017 - Mois européen de la cybersécurité

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

TABLE DES MATIERES

OBJET DU DOCUMENT

Les grandes organisations comme les gouvernements se dotent naturellement des moyens protégés de transmissions. Ils leur permettent d'assurer des échanges de documents sensibles de manière confidentielle. Dès qu'ils sont disponibles entre les parties, il convient de les utiliser en priorité.

Dans les cas où ils ne sont pas disponibles ou utilisables (pas déployés sur le site, sur l'ordinateur, pas de clés partagées au préalable, etc.), les utilisateurs sont parfois livrés à eux-mêmes alors qu'en utilisant des moyens courants à leur disposition, ils pourraient déjà protéger leurs informations de façon très efficace.

Autrement dit, ce document est un guide de pratiques pour éviter des expositions inutiles, quand un peu de sécurité opérationnelle vaut mieux qu'une sécurité théorique mais hypothétique, quand on ferme un verrou multipoint à défaut d'une porte blindée (qui exigerait d'avoir renforcé le mur)

Ce document ne se substitue pas aux conditions réglementaires prévues par divers environnements, activités ou professions (PCI DSS, IGI.1300 ou autres). Il peut être utilisé pour la gestion d'un dossier ou document « sensible », sans que cet adjectif ait une définition juridique mais que chacun comprend comme tout ce qu'on n'a pas envie de voir divulguer en public. En particulier, les mesures décrites ci-après sont une manière de répondre au besoin de protéger des « secrets des affaires ».

RISQUES

Dans ce contexte, le risque contre lequel on cherche à se prémunir est celui de **documents ou fichiers « nus » ou « en clair** », quel que soit le support, clé USB, dossier de courriels, répertoire partagé. Sans protection par chiffrement, une personne qui a accès en lecture peut prendre connaissance du fichier.

Un second risque associé est celui de **fichiers chiffrés mais insuffisamment protégés, notamment par l'emploi d'un secret trop faible**. Par exemple, le mot de passe est trivial ou a une complexité (entropie) insuffisante. Si un utilisateur génère un code lui-même de tête, il est possible de prédire statistiquement le prochain caractère d'une chaîne quand on connaît les 2 précédents par exemple. Les meilleurs « craqueurs » de mots de passe explorent l'espace des mots de passe en suivant un modèle de Markov. Leurs résultats sur des mots de passe générés par un utilisateur (et non un algorithme) sont excellents, même sur des mots de passe de 10, 12 voire 15 caractères.

La sécurité d'un mot de passe peut aussi être affaiblie par le réemploi dans un contexte différent où il est moins bien protégé.

RECOMMANDATIONS PRATIQUES

Utiliser un gestionnaire de mots de passe

La première mesure consiste à utiliser des gestionnaires de mots de passe pour générer et stocker les mots de passe ou les phrases de passe.

Il est de la responsabilité des DSI de mettre à disposition[1] de leurs utilisateurs, des gestionnaires sur PC fixe et aussi sur ordiphones (les utilisateurs les conservent toujours sur eux, se rendent compte et signalent rapidement leur perte ou leur vol).
Il est recommandé d'utiliser des outils ayant des formats de fichiers (et donc d'algorithmes) documentés, faisant l'objet de plusieurs implémentations. Les filières open source KeePass http://keepass.info/ [2] et PasswordSafe https://pwsafe.org/ répondent à tous ces critères.

NB : en 2011, l'ANSSI a attribué la certification CSPN à une ancienne version de KeePass, confirmant des bases cryptographiques saines
https://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/

Générer des secrets forts

Les gestionnaires de mots de passe possèdent généralement un indicateur d'entropie ou de complexité. Un équivalent d'entropie de 128 bits est nécessaire pour résister aux attaques par dictionnaires selon les meilleures techniques actuelles (grappes de GPU).
Certains outils sont capables de générer des « phrases de passe ». A entropie équivalente, elles sont aussi fortes mais plus faciles à saisir sur un clavier pour un utilisateur (voire pour les plus forts à mémoriser).

Distribuer un carnet de codes

Pour pourvoir échanger des documents, un carnet de mots de passe est à distribuer aux acteurs en début de projet, ou lors de la première réunion annuelle du cercle de confiance. Le gestionnaire du carnet de codes tient un inventaire des personnes auxquelles il a distribué un exemplaire.

Un schéma simple mais efficace consiste à définir **un mot de passe par mois** dans le carnet de code. Les utilisateurs au sein du cercle de confiance sélectionnent le code du mois pour le fichier / document qu'ils veulent protéger. Pour faciliter les opérations, il est de bonne pratique d'inclure la date dans le nom de fichier, par exemple avec un préfixe au format AAMMJJ.

L'utilisation d'un mot de passe mensuel limite la zone d'impact si un code venait à être divulgué.

---

[1] Il n'est pas nécessaire d'installer au sens plein du terme puisque les outils identifiés ci-après ne réclament pas de droit d'administration sur un équipement.
[2] https://play.google.com/store/apps/details?id=keepass2android.keepass2android_nonet&hl=fr , https://itunes.apple.com/fr/app/minikeepass-secure-password-manager/id451661808?mt=8 et https://www.keepassx.org/ pour des versions respectivement pour Android, iOS et Linux

Chiffrer nativement les documents eux-mêmes

Depuis que les Etats-Unis ont dérèglementé l'exportation de moyens de chiffrement fort au tournant des années 2000, les formats de fichiers modernes ont des moyens natifs de protection à l'état de l'art.
En général, la clé de chiffrement est dérivée du code de passe saisi par l'utilisateur par PBKDF2 (password based key derivation function 2, qui consiste essentiellement en l'application de multiples fois d'un algorithme de hachage, le nombre de répétitions est défini en fonction de la puissance de calcul de référence du moment). Le chiffrement par bloc est assuré par AES, ce qui permet de disposer des jeux d'instructions natives des processeurs.

Correspondent à cet état de l'art les formats .docx, .xsls, .odt et .pdf

Les conteneurs .zip sont capables des mêmes performances mais par exemple 7zip favorise par défaut la compatibilité (et un chiffrement faible et donc une protection illusoire) par rapport à l'état de l'art de la sécurité. Il faut donc être attentif quand on l'utilise.

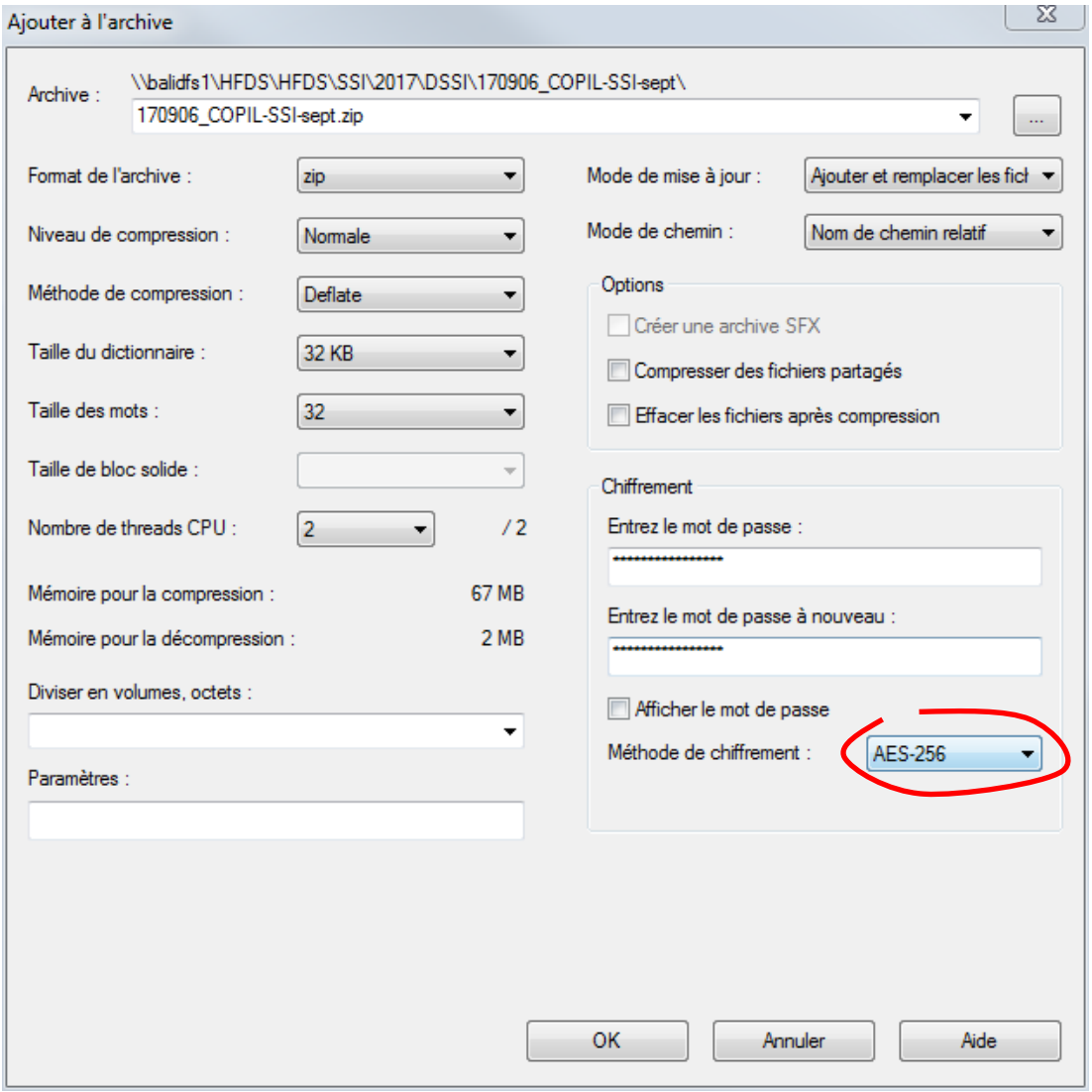

Figure 1 : réglage sécurisé de 7-zip

De plus, l'ouverture d'un .zip risque de laisser des fichiers temporaires sur le poste de travail, contrairement au chiffrement du document lui-même. Ce dernier scénario est donc à privilégier.

Utiliser des noms de code

Parfois l'information à protéger est déjà contenue dans le nom du projet, du dossier. Par exemple, le nom de la société ciblée dans le cadre de fusion/rachat d'entreprises.

Face à des volumes d'échanges importants, les dispositifs de recherche automatisée repèrent des mots clés. Une façon simple et presque ludique de gêner leur action consiste à utiliser un nom de code courant, particulièrement un nom de lieu géographique, touristique si possible. Ce type de noms de code s'inscrit naturellement dans des phrases, et est facilement mémorisable.

Le choix de ce nom de code est à faire soit en début de projet, soit dès que le dossier commence à être identifié comme sensible.

EN RESUME

Il est aisé de protéger des documents avec des moyens existants sur tout poste de travail.

Le seul « coût » à payer est celui des quelques minutes de formation pour se familiariser avec les outils et quelques secondes de manipulation à chaque ouverture de document. Pour des usages plus intensifs, il existe des solutions plus sophistiquées qui permettent plus de « transparence » en usage courant.

Dans tous les cas, si l'organisation a réellement à cœur de protéger des informations qu'elle juge sensibles (ce qui implique un travail de classification car tout document ne mérite pas le même niveau de protection), elle en a l'opportunité et le choix.

Contact : dssi.shfds (at) finances.gouv.fr
Diffusion Internet : https://www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi

HFDS Bercy