Pourquoi et comment chiffrer ses données ?

Dernière modification : 06 avril 2022

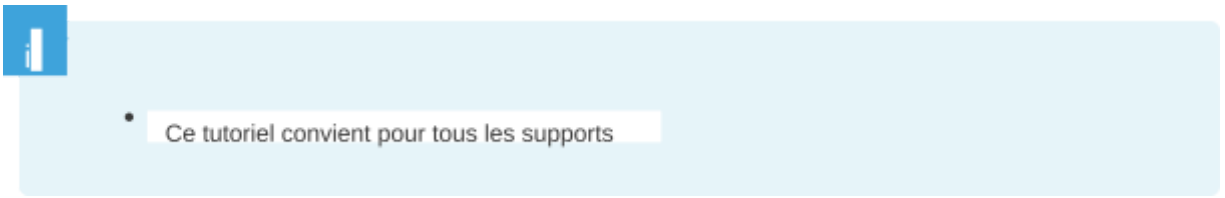
Tags

#chiffrement #cryptographie #confidentialité #sécurité

Résumé

Le chiffrement est une technique pour garantir l'authenticité et préserver la confidentialité ainsi que l'intégrité de données confidentielles et sensibles.
Ce tutoriel a pour objectif de présenter l'intérêt de chiffrer ses données, et comment les chiffrer.

Prérequis



Dans quels cas ?

Le chiffrement est intéressant, voire nécessaire, dans certaines situations personnelles ou professionnelles :

Je dois **envoyer par e-mail un document confidentiel** et sensible à un client ou à un partenaire
Je dois **transporter des documents administratifs sur une clé USB** ou un disque dur externe
Je me déplace beaucoup avec **mon ordinateur portable** qui **contient des informations**
stratégiques **importantes pour mon activité**
Je veux **accéder à un fichier** avec des données personnelles **depuis le cloud**
Je veux **signer numériquement un e-mail** pour valider son authenticité

Le chiffrement et les techniques cryptographiques peuvent réduire l'impact en cas de vol de données et renforcer la sécurité de données sensibles.

Le chiffrement de document

Il existe plusieurs possibilités de chiffrer ces documents ou ces dossiers, voire un disque entier : **les logiciels de compression, les services en ligne et les logiciels dédiés**.

Les logiciels de compression

Des logiciels pour compresser des documents proposent une option chiffrement avec un déchiffrement par mot de passe (WinRAR, WinZIP ou 7-Zip).

S'ils semblent être un bon compromis entre sécurité et simplicité, il faut rester vigilant car la sécurité de vos documents n'est pas le but premier.
Les algorithmes qu'ils emploient sont ou peuvent devenir obsolètes et donc non sécurisés dans le temps.

Les services en ligne et les logiciels dédiés

Des services en ligne chiffrent des données tels que Hat.sh.

Des logiciels plus spécifiques tels que Zed! créent des conteneurs sécurisés pour vos documents, VeraCrypt chiffre des volumes de données entiers, tels qu'une clé USB ou un disque dur externe. Il existe aussi d'autres logiciels dédiés comme Encrypto.

Si vous possédez une version professionnelle de Windows 10, Bitlocker est le système de chiffrement natif proposé par Microsoft.

Le chiffrement dans le cloud

Sur les espaces de stockage cloud (Google Drive, Microsoft OneDrive, Dropbox...), les données sont chiffrées côté serveur. Concrètement, vos données sont protégées en cas de vol d'un disque dans un datacenter et lors de leur transmission entre votre ordinateur et les serveurs cloud.
Si une personne pirate vos identifiants et accède à votre espace de stockage, elle pourra lire tous les fichiers stockés.
Il est recommandé de chiffrer en amont avec l'une des techniques présentées dans la partie précédente.
Des solutions dédiées pour le cloud sont également disponibles telles que Boxcryptor ou Cryptomator.
Sur OneDrive, le Coffre-fort Personnel (ou Personal Vault stocke des fichiers avec plus de sécurité. Il ne s'agit pas d'un chiffrement en soi, mais son accès nécessite de vérifier son identité avec son téléphone.

Le chiffrement des e-mails

Pour protéger un e-mail, il est nécessaire de sécuriser la connexion entre votre ordinateur et le serveur de messagerie, et de chiffrer l'e-mail lui-même.
La sécurité de la connexion entre l'ordinateur et le serveur de messagerie passe par le chiffrement de cette connexion avec le protocole SSL/TLS. C'est le fameux "S" du HTTPS que vous voyez lorsque vous vous connectez sur un client mail en ligne.
Les principaux fournisseurs de services de messagerie le proposent par défaut, pour chiffrer la connexion entre votre ordinateur et le serveur de messagerie.
Mais une personne ayant accès à vos identifiants pourrait lire vos e-mails. Il faudrait, dans ce cas, chiffrer l'e-mail.
Pour cela, le chiffrement de bout en bout opère avec des protocoles tels que S/MIME ou PGP/MIME.

Ces systèmes assurent une sécurité complémentaire : si une personne pénètre votre messagerie, mais qu'elle ne possède pas la clé de déchiffrement pour le mail, elle ne pourra pas lire ces e-mails privés.
Des logiciels comme Gpg4Win pour Windows par exemple appliquent le protocole PGP.
Des extensions de navigateur tels que FlowCrypt sur Google Chrome sont prévues pour ce type de protocole sur un client web.

Pour aller plus loin - liens utiles

CNIL – Comment chiffrer ses documents et ses répertoires

CNIL – Comprendre les grands principes de la cryptologie et du chiffrement

Globalsign – Qu'est-ce que le S/MIME, comment ça marche ?

Licence

Ce tutoriel a été produit dans le cadre du projet Clic&Connect.
L'objectif est d'accompagner les petites structures économiques dans leurs besoins d'acquisition d'outils numériques et de leur permettre d'accéder aux dispositifs publics mis en place visant à maintenir, développer et pérenniser l'activité des TPE.