Le chiffrement des données

Derrière cette obscure expression se cache une solution efficace pour protéger vos données les plus sensibles. Elle vous évite le pire si vous perdez votre PC portable ou une clé USB.

Il n'est pas nécessaire d'être un crac du piratage pour récupérer des informations confidentielles sur une entreprise. Les salons professionnels font en effet le bonheur de concurrents un peu trop curieux. Il suffit de ramasser discrètement une clé USB ou de tomber par « hasard » sur un PC portable (ou un smartphone) pour mettre la main sur de précieux fichiers. La tâche est un jeu d'enfant si ces appareils mobiles ne sont pas sécurisés (voir notre fiche sur le BYOD) !

Par contre, cette opération devient un casse-tête si justement vous avez « chiffré » les documents sensibles qu'ils contiennent. Plus connue sous le terme de « cryptage », cette méthode consiste **à protéger vos fichiers en les rendant illisibles par toute personne n'ayant pas la clé dite de déchiffrement.** Sans le bon mot de passe, le contenu reste inaccessible.

Malheureusement, cette pratique est loin d'être généralisée. « La moitié des données stockées dans Google Drive sont partagées avec des utilisateurs situés à l'extérieur de l'entreprise », constate Bitglass, spécialiste américain de la protection totale des données, dans son étude parue en septembre 2017. Or, l'absence de chiffrement expose les entreprises à des fuites d'informations ou à des modifications malveillantes des données.

Pourquoi chiffrer ses documents et ses répertoires ?

- **Pour renforcer la sécurité de vos données**
  Le chiffrement assure la confidentialité de vos projets les plus importants pour votre activité économique, mais également la sécurité des données à caractère personnel que vous stockez en interne, chez un prestataire informatique ou dans le Cloud. Ce procédé cryptographique permet également d'assurer l'intégrité d'une information (elle ne peut pas être modifiée).

- **Pour limiter les effets négatifs d'une perte de données**
  Si une personne perd ou se fait voler son ordinateur portable lors d'un déplacement, les conséquences seront réduites, car ses dossiers importants seront chiffrés.

Le chiffrement des données : les principales mesures à prendre

- **Première mesure : chiffrer les données confidentielles**
  Tout répertoire comportant des informations sensibles ou à caractère personnel doit être chiffré. Cette technique permet en effet de restreindre les accès et de disposer de preuves en cas de fuite de données. Cette mesure concerne aussi bien les dossiers en interne ou stockés dans le Cloud.

- **Deuxième mesure : chiffrer des e-mails**
  Un courrier électronique non « crypté » c'est comme une carte postale : tout le monde peut le lire. Il est transmis en « clair ». En étant chiffré, un e-mail ne pourra être lu que par le destinataire disposant de la bonne clé. Attention, ce procédé « masque » le contenu et la pièce jointe, mais pas l'intitulé du message. Évitez d'indiquer des termes trop explicites… Cette technique permet aussi d'authentifier un e-mail en le signant.

- **Troisième mesure : chiffrer les appareils mobiles**
  Les salariés voyageant beaucoup à l'étranger ou se rendant dans des salons professionnels doivent posséder un PC portable et/ou un smartphone dont le disque dur est chiffré entièrement ou partiellement (seuls quelques dossiers sont protégés).

Ce qu'il ne faut pas faire

Utiliser n'importe quelle solution de chiffrement

Il existe de très nombreuses solutions cryptographiques. Mais **elles ne bénéficient pas toutes de vérifications assurées par des experts ou certifiées par l'ANSSI** (Agence nationale de la sécurité des systèmes d'information).

Par exemple, si vous envisagez d'utiliser le logiciel Truecrypt pour chiffrer des documents ou des dossiers, une seule version (la 6.0a) est reconnue par l'Agence de sécurité des systèmes d'information.

Pour aller plus loin

La signature électronique : la dématérialisation sécurisée

Adoptée par l'Assemblée nationale le 29 février 2000 (décrets d'application parus le 30 mars 2001), la signature électronique donne à un e-mail ou à un document électronique (contrats, mandats de prélèvement SEPA...) valeur de preuve au même titre que la feuille de papier. Mais l'article 1366 du Code civil français précise : « sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ». Vous devez donc vous adresser à un tiers de confiance (agréé et certifié) qui mettra à disposition les outils que vous utiliserez pour signer.

Votée en 2016, la loi Lemaire rend possible l'envoi d'un recommandé électronique à une administration (article 93, III). Cette disposition codifiée à l'article L. 112-15 du code des relations entre le public et l'administration a fait l'objet d'un décret d'application paru dans le Journal officiel du 23 décembre 2017.

LEXIQUE

Un système à clé publique (ou asymétrique) est un système cryptographique qui utilise deux clés, une clé publique et une clé secrète :

- **la clé publique :** librement publiable, elle est nécessaire à la mise en œuvre du chiffrement. Elle peut également servir à vérifier les signatures électroniques réalisées par la clé privée associée ;
- **la clé privée :** gardée confidentielle par son détenteur, elle sert à « signer » des données et à déchiffrer celles chiffrées par la clé publique associée.

Generali IARD, Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris. N° d'identifiant unique ADEME FR232327_01NBYI.
Siège social : 89 rue Taitbout - 75009 Paris.
Société appartenant au Groupe Generali immatriculé sur le registre italien des groupes d'assurances sous le numéro 026.

SG2685MARK-25 - Décembre 2025 - Studio graphique