BlueFinch ESB

Comprendre les enjeux du chiffrement pour sécuriser les données de votre entreprise

SOMMAIRE

1. Introduction

La digitalisation de nos activités est devenue en quelques années indispensable au développement économique des entreprises, organisations ainsi qu'aux administrations en charge de la gestion des services publics des états.

Le corollaire de cette digitalisation à grande vitesse de nos processus d'échanges de données - aussi bien internes qu'externes - est qu'elle ouvre toute grande la porte à un « Far West » numérique. Le cyberespace est devenu le terrain de chasse d'une nouvelle forme de délinquance en col blanc pouvant être affiliée à des états voyous ou à des groupes indépendants.

De ce fait, le nombre de cyberattaques a explosé et elles sont malheureusement encore souvent mésestimées aussi bien des entreprises que du grand public. C'est donc à une véritable « guerre » qui ne dit pas son nom à laquelle nous assistons.

Si la cybersécurité est devenue une préoccupation constante dans les entreprises, elle n'en reste pas moins encore à améliorer et à renforcer tant la cybercriminalité devient de plus en plus dommageable.

Selon Statista[1] , les principales faiblesses en matière de sécurité sont dues :

- Au nombre trop important de données gérées dans les entreprises,
- Au manque de personnel IT qualifié,
- Au manque de connaissances en matière de bonnes pratiques et de cybersécurité par les collaborateurs,
- A l'impossibilité de combiner les solutions de sécurité entre elles.

Ce livre blanc a pour objet d'apporter un éclairage sur le chiffrement qui reste un composant encore peu mis en œuvre dans une stratégie de cybersécurité.

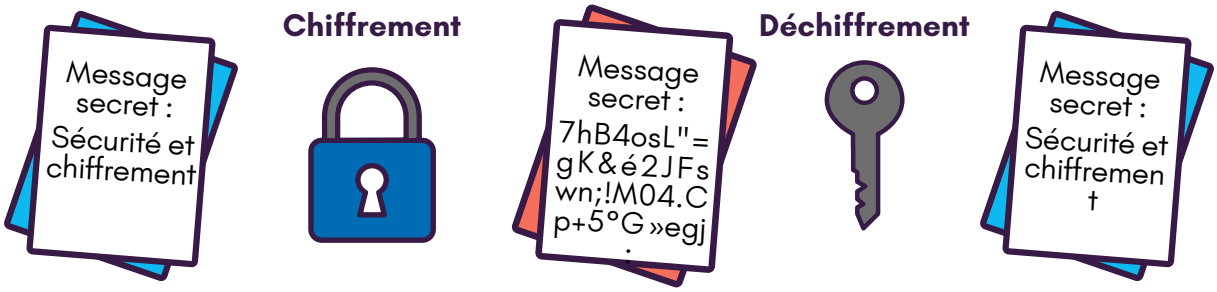
C'est un procédé ancestral utilisé pour dissimuler des informations confidentielles et qui trouve tout son sens à l'ère du tout numérique.

1 https://www.statista.com/

2. Qu'est-ce que le chiffrement ?

Le principe du chiffrement est assez simple. Il répond à un besoin de dissimulation d'une information, ou de nos jours, de données sensibles et personnelles aux personnes qui ne sont pas habilitées à les voir. Le chiffrement permet donc de rendre les informations totalement incompréhensibles afin d'en garder la confidentialité. Il existe depuis plusieurs millénaires, consistant à encoder une information que seul le destinataire peut déchiffrer.

Le chiffrement s'appuie sur un mécanisme cryptographique (d'écriture secrète), utilisant des algorithmes mathématiques sophistiqués. C'est un processus réversible qui masque les données. Il est donc toujours possible de retrouver leur valeur initiale grâce à une clé. Cette clé, qui est une opération cryptographique de déchiffrement, va permettre de verrouiller et déverrouiller le chiffrement des informations.



3. A quoi sert le chiffrement et pour qui est-il essentiel ?

Le chiffrement est aujourd'hui indispensable pour assurer la protection des données, permettre des échanges sûrs et lutter contre les risques liés aux fuites de données. Recommandé par la CNIL[2] concernant le règlement général de protection des données (RGPD), il contribue à faire de la cybersécurité le « vecteur de confiance et d'innovation », en plus d'être devenu un enjeu majeur pour protéger les informations des entreprises et citoyens Européens. L'objectif du chiffrement est de garantir la confidentialité des données échangées pendant leur transfert et leur stockage.

Le chiffrement est utilisé par différents secteurs d'activité, notamment dans les domaines de la santé, de la finance, des ressources humaines, de l'éducation, des administrations, du développement, etc.

L'objectif du chiffrement consiste à ce que les données/fichiers ne soient pas utilisables en dehors de l'application en cas de vol, copie, perte ou téléchargement. L'enjeu du chiffrement est donc de protéger les données sensibles. Toutefois, il vise également à maintenir la confiance des utilisateurs dans la sécurité

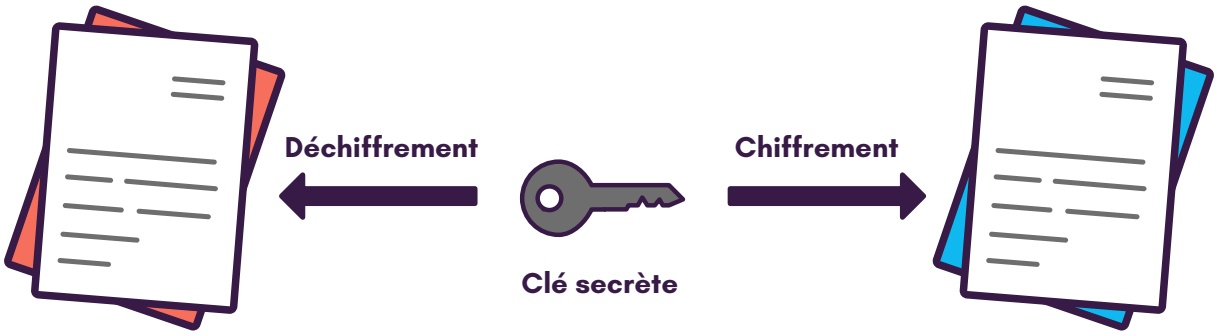
Le saviez-vous ? *Le terme « cryptage » n'est pas reconnu par le dictionnaire de l'Académie française. En effet, la terminologie de cryptage reviendrait à coder un fichier sans en connaître la clé et donc sans pouvoir le décoder ensuite.*

2 https://www.cnil.fr/

4. Les différents types de chiffrement

On distingue 2 principaux types de chiffrement de données : le chiffrement symétrique et le chiffrement asymétrique. Ces 2 types de chiffrement diffèrent au niveau de la façon dont les données sont déchiffrées.

- **Le chiffrement symétrique (ou à clé privé) :** lorsqu'on utilise ce chiffrement, il s'agit de la même clé est qui est utilisée pour chiffrer ou déchiffrer un message ou un fichier. Bien que ce chiffrement symétrique soit rapide, il peut vite s'avérer fastidieux dans la gestion et distribution de grandes quantités de clés nécessaires aux destinataires pour chaque déchiffrement.



- **Le chiffrement asymétrique (ou à clé publique) :** lors du chiffrement de données asymétriques, deux clés sont utilisées : une clé publique et une clé privée. La clé publique peut être partagée avec n'importe qui, mais la clé privée doit impérativement être protégée.

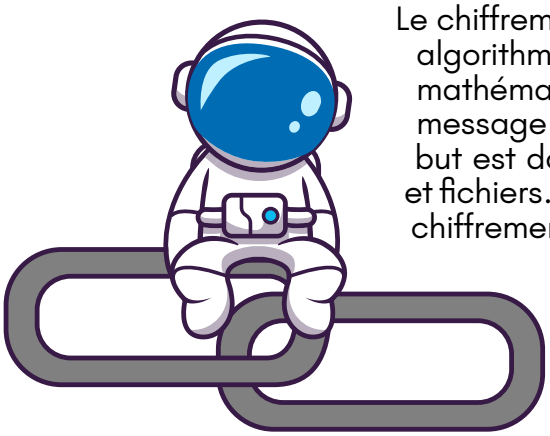
Il existe une technique combinant chiffrements symétrique et asymétrique appelée « chiffrement hybride ». Cette technique permet de déterminer une clé secrète par l'une des deux parties souhaitant communiquer. La clé est alors envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, ces clés communiquent en chiffrant symétriquement leurs échanges.

5. Les algorithmes et mécanismes

Le chiffrement provient de la science appelée cryptologie. La cryptologie combine l'étude de l'écriture secrète (la cryptographie) et l'analyse des attaques contre les mécanismes de cryptographie (la cryptanalyse).

La cryptologie englobe différentes fonctions de sécurité, dont le chiffrement. Ces fonctions de sécurité sont dotées d'algorithmes qui les composent. Chaque fonction de sécurité assure une mission différente de protection des données et des transferts de fichiers.

A. Le chiffrement



Le chiffrement est une première fonction de sécurité. Les algorithmes de chiffrement, c'est à dire les processus mathématiques, transforment, à l'aide d'une clé, un message en clair en un message incompréhensible. Son but est donc d'assurer la confidentialité des messages et fichiers. Comme vu précédemment, il existe 2 types de chiffrement : symétrique et asymétrique.

Le facteur le plus courant qui favorise un chiffrement plutôt qu'un autre est son algorithme. Ce sont le plus souvent la vitesse d'exécution, la fiabilité et la sécurité des algorithmes qui font pencher la balance du choix d'un chiffrement.

Voici une liste d'algorithmes de chiffrement symétrique et asymétrique les plus connus.

AES - Advanced Encryption Standard est un algorithme de chiffrement symétrique. Il est l'algorithme le plus utilisé et le plus sûr. Il est pratiquement implanté dans tous les logiciels qui chiffrent les données.

Serpent est un algorithme de chiffrement symétrique tout aussi sûr que AES.

Blowfish est un algorithme de chiffrement symétrique. Rapide d'exécution, il est pourtant de plus en plus déprécié en raison de sa taille de blocs (nombre de bits présents). Il a été placé dans le domaine public par son créateur (pas de brevet ni de licence).

Twofish est un algorithme de chiffrement symétrique basé sur Blowfish. Twofish a été conçu pour être implanté dans des cartes à puce et d'autres systèmes embarqués. Complexe, il reste cependant peu utilisé malgré sa robustesse.

Triple DES est un algorithme de chiffrement symétrique dérivé de DES (Data Encryption Standard), algorithme de chiffrement symétrique devenu obsolète à cause de sa lenteur. Celui-ci est de moins en moins utilisé, remplacé par AES.

RSA est un algorithme de chiffrement asymétrique très utilisé pour échanger des données sensibles. Il utilise une paire de clés composée d'une clé

B. Le hachage

La fonction de hachage a pour objectif de garantir l'intégrité des données. Composé lui aussi de différents algorithmes, le hachage est un processus irréversible qui génère une chaîne de caractères toujours de la même longueur, peu importe la taille du texte brut.

Voici 2 exemples de hachage :

- **SHA-0/1/2/3** - Secure Hash Algorithme est un type de hachage cryptographique. Cependant SHA-0 et SHA-1 sont de moins en moins utilisés depuis l'apparition de plusieurs failles. Ils laissent leurs petits frères SHA-2 et SHA-3 prendre le relai.
- **Whirlpool** - La fonction utilise une architecture robuste à la cryptanalyse. Son utilisation est complètement libre, aucun brevet ne limite son emploi.

C. La signature numérique

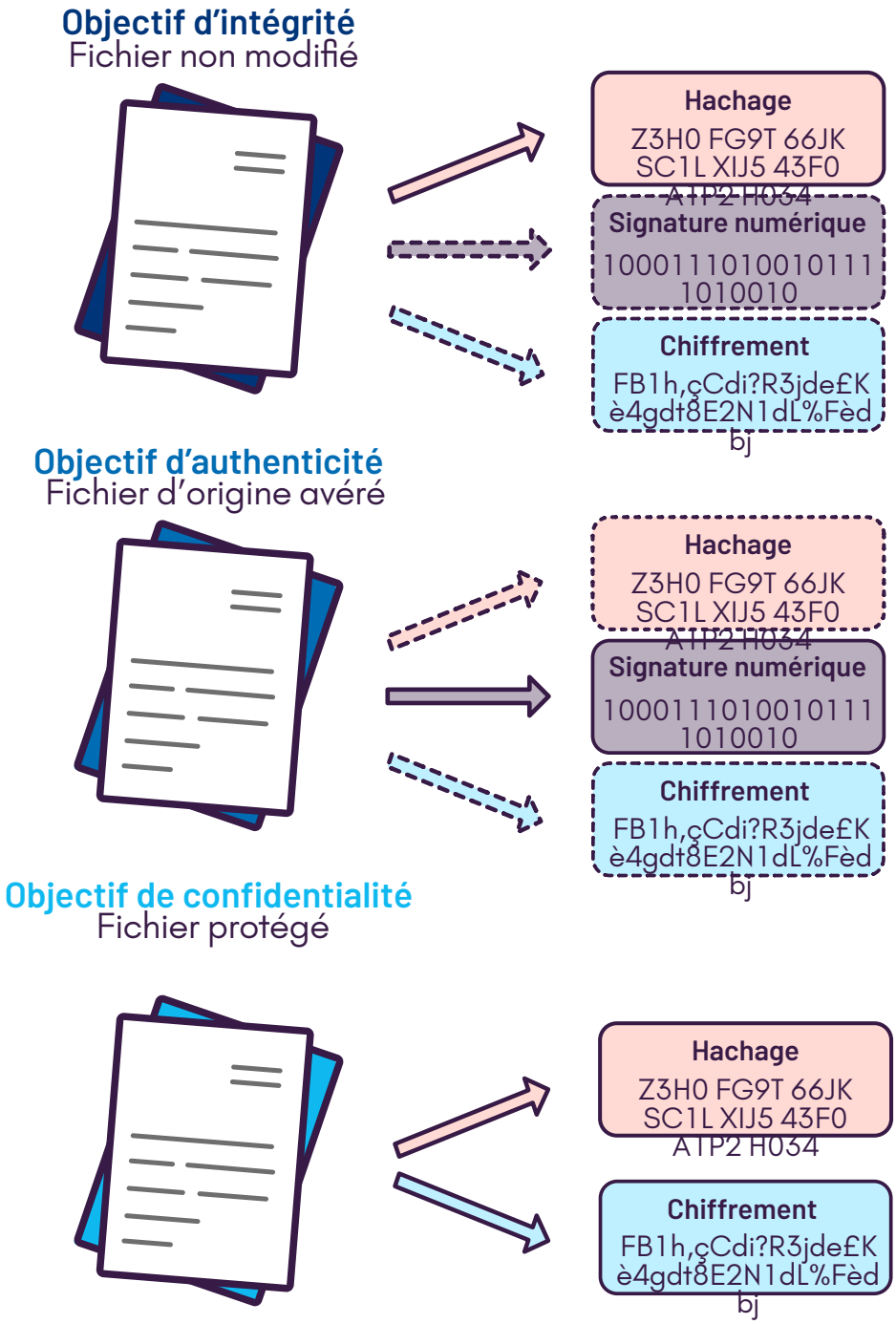
Pour assurer l'authenticité d'un message, c'est la signature numérique qui est utilisée. Non visible, elle permet d'être sûr de l'origine d'un fichier en authentifiant l'émetteur.

La signature numérique s'appuie généralement sur la cryptographie asymétrique et le hachage. Il n'y a donc pas d'algorithmes propres à la signature numérique.

D. Pour résumer

La cryptologie encadre différents objectifs de sécurité en s'appuyant sur différents mécanismes.

Par ailleurs, bon nombre d'algorithmes de chiffrement ou de hachage sont faits maison. Lorsqu'ils sont peu connus et éprouvés, ils sont beaucoup moins utilisés. Cependant, ils n'en restent pas obligatoirement moins fiables.



6. Les logiciels de chiffrement

Il existe une multitude de logiciels de chiffrement. Les logiciels les plus performants et répandus sont issus généralement de logiciels libres. Pourtant, tous les logiciels n'ont pas le même objectif et ne sont pas faits pour tous les mêmes types de systèmes d'exploitation (Mac OS, LINUX, Windows, IBM i, etc.). Certains logiciels assurent le chiffrement de courriels ou de fichiers, d'autres de disques durs ou encore la communication sécurisée entre plusieurs ordinateurs. Ces logiciels utilisent généralement un protocole de chiffrement lorsqu'il s'agit de sécuriser les communications.

En somme, le logiciel est l'exploitation de différents éléments formant un logiciel de

Voici quelques tips de logiciels courants.

PGP – Pretty Good Privacy est une famille de systèmes logiciels de chiffrement développée par Philip R. Zimmermann à partir duquel OpenPGP est basé.

PGP est utilisé pour le chiffrement et déchiffrement de courriels et de fichiers. Il utilise la cryptographie asymétrique et symétrique.

Il fait partie des logiciels de chiffrement hybride et est le plus connu.

Attention à ne pas confondre avec OpenPGP qui est une méthode de cryptographie qui fournit des services d'intégrité des données pour les messages et les fichiers. OpenPGP est un standard dit Open Source permettant d'utiliser PGP dans des logiciels.

OpenPGP combine le chiffrement à clé symétrique et le chiffrement à clé publique pour assurer la confidentialité.

GnuPG – The GNU Privacy Guard est un logiciel libre provenant du standard OpenPGP. Il permet de chiffrer et signer les communications. Il dispose d'un système de gestion de clés polyvalent, ainsi que de modules d'accès pour toutes sortes de répertoires de clés publiques.
Site -> https://www.gnupg.org/index.fr.html

AxCrypt – Logiciel de chiffrement gratuit sur Windows, il permet le chiffrement de fichiers grâce à l'algorithme AES. Il est également possible de transmettre des fichiers protégés sans obligation d'utilisation AxCrypt.
Site -> https://www.axantum.com/

7-Zip – Logiciel qui permet de compresser un ou plusieurs documents et de les chiffrer. Il exploite l'algorithme AES. Bien que non comparable à des poids lourds comme GnuPGP, il est néanmoins très commun et utile. De plus, il est gratuit et téléchargeable.
Site -> https://www.7-zip.org/

Il existe bien évidemment beaucoup d'autres logiciels libres répondant à différentes problématiques de chiffrement.

7. Qu'est-ce qu'un protocole de chiffrement ?

Un protocole de chiffrement est un moyen sûr de transmettre des renseignements. Il fonctionne conjointement avec les protocoles de transferts (comme HTTPS, AS2, FTPS, etc.) et les algorithmes de chiffrement et/ou de hachage. C'est ce « tout » qui permet la sécurisation optimale lors d'une communication.

Voici quelques exemples de protocole de chiffrement :

SSH - Secure Shell est un protocole de communication mais aussi un programme informatique. Le protocole est utilisé pour un établir un accès sécurisé afin d'effectuer des opérations sensibles sur des machines distantes et des transferts de fichiers à travers un réseau ouvert tout en garantissant l'authentification, la confidentialité et l'intégrité des données.

SSH est prévu pour fonctionner avec un grand nombre d'algorithmes de chiffrement.

SSL et TLS - Secure Socket Layer est un protocole utilisé pour la sécurisation des échanges entre clients et serveurs. Il est utilisé avec TCP, protocole de transport et l'application correspondant aux protocoles SMTP, HTTP ou FTP.

Le protocole SSL assure conjointement les fonctions sécuritaires d'authentification, de confidentialité et d'intégrité. La confidentialité repose sur des algorithmes de chiffrement symétrique comme AES, DES, triple DES, etc. L'intégrité des données est assurée par l'utilisation du hachage de type SHA.

Toutefois, SSL est de plus en plus abandonné au profit de TLS pour faire face aux vulnérabilités. Son successeur « Transport Layer Security », prend en charge des suites et des algorithmes de chiffrement plus forts et plus sécurisés.

S/MIME - Cette méthode de chiffrement exige que les systèmes de courrier électronique de l'expéditeur et du destinataire prennent en charge les communications S/MIME. L'expéditeur doit créer un certificat et l'envoyer au destinataire. Le destinataire devra ensuite importer le certificat dans son Client de messagerie. Une fois le certificat en place, un courrier électronique sécurisé peut être envoyé, reçu et déchiffré.

8. Quels sont les bénéfices du chiffrement de données ?

A. La sécurité

Le chiffrement est une première fonction de sécurité. Les algorithmes de chiffrement, c'est à dire les processus mathématiques, transforment, à l'aide d'une clé, un message en clair en un message incompréhensible. Son but est donc d'assurer la confidentialité des messages et fichiers. Comme vu précédemment, il existe 2 types de chiffrement : symétrique et asymétrique.

Le facteur le plus courant qui favorise un chiffrement plutôt qu'un autre est son algorithme. Ce sont le plus souvent la vitesse d'exécution, la fiabilité et la sécurité des algorithmes qui font pencher la balance du choix d'un chiffrement.

Voici une liste d'algorithmes de chiffrement symétrique et asymétrique les plus connus.

B. La conformité

Les entreprises ont souvent le choix parmi une multitude de normes de chiffrement. Cependant, les réglementations et exigences spécifiques, les orientent vers certains types de mesures de chiffrement des données plutôt que d'autres. Vérifiez bien l'adéquation du logiciel du chiffrement avec les normes de conformité exigées dans votre entreprise.

Plusieurs réglementations recommandent le chiffrement des données :

RGPD – Le règlement Général de la Protection des Données encadre le traitement des données personnelles sur le territoire de l'Union européenne et la préservation des droits de chacun. *« Le règlement affirme ainsi l'importance d'apprécier et traiter les risques sur les personnes. Il exige notamment des entités concernées, la mise en œuvre de « mesures techniques ou organisationnelles appropriées », qui peuvent notamment inclure le « chiffrement des données » et des « moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience »*[3].

HIPAA - Health Insurance Portability and Accountability Act : La loi HIPAA est une réglementation Américaine en matière de gestion de dossiers médicaux. Toutes les entreprises ou prestataires de santé qui manipulent des renseignements médicaux sensibles doivent veiller à la sécurité et à la consignation de tous les renseignements médicaux à caractère identifiable.
C'est pourquoi le chiffrement fait partie des prescriptions de cette réglementation. Il permet de chiffrer toutes les informations identifiables pour protéger les patients et entreprises d'éventuels incidents de cybersécurité.

LPD – Loi fédérale sur la Protection des Données : *« En Suisse, toute opération en relation avec des données personnelles est soumise à la LPD : les données doivent être traitées dans le but pour lequel elles ont été collectées, elles doivent être détruites une fois le traitement effectué, la personne doit avoir été informée du but du traitement et y avoir consenti. L'exactitude des données et leur sécurité doivent être garanties. Le droit d'accès aux données doit être garanti à la personne concernée.»*[4] Ressemblant fortement au RGPD, le chiffrement est là aussi un outil de sécurisation important pour protéger les données.

PCI DSS - Payment Card Industry Data Security Standard : C'est une norme de sécurité internationale concernant les cartes de paiement afin de réduire l'utilisation frauduleuse des outils de paiement. Le standard spécifie 12 conditions de conformité, dont le chiffrement de la transmission des données du titulaire et de protéger les données stockées.

3 Source : https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/
4 Source : https://libguides.graduateinstitute.ch/

9. Quels sont les risques liés au chiffrement ?

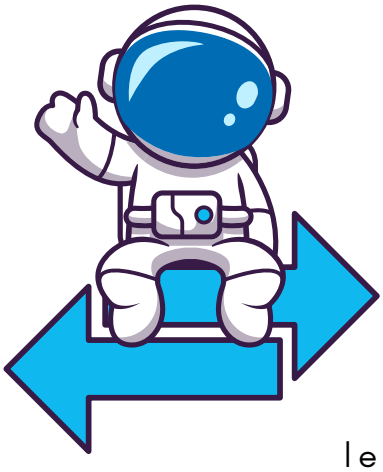
Beaucoup de hackers tentent de déchiffrer les données. Ils utilisent souvent la méthode de l'attaque par force brute. Cette dernière consiste à essayer de multiples clés au hasard jusqu'à ce que l'une d'entre elles fonctionne. C'est pourquoi, il est recommandé d'utiliser des clés longues pour réduire le pourcentage de chances que la bonne clé soit trouvée de cette façon.

Ils utilisent également la technique de la cryptanalyse qui consiste à trouver une faiblesse dans le chiffrement et à l'exploiter. Cette technique peut fonctionner lorsqu'une faille est présente dans le chiffrement en lui-même.

Bien souvent, il ne s'agit pas du chiffrement à proprement parler qui est « corrompu », mais des failles ou erreurs du système autour.

10. Le chiffrement et la sécurité des transferts de fichiers

Il est impératif en entreprise que les données soient chiffrées lorsqu'elles sont en transit vers un destinataire et lorsqu'elles sont au repos, c'est-à-dire stockées sur un serveur.



Il s'agit de l'une des pratiques les plus importante pour votre sécurité informatique.

Certaines équipes IT utilisent des outils OpenPGP gratuits pour assurer la sécurité des fichiers, tandis que d'autres optent pour une solution professionnelle de transferts de fichiers pour protéger les données.

Les solutions de transferts de fichiers automatisent le processus de chiffrement, garantissant ainsi la sécurité des fichiers. Elles permettent aussi de choisir le protocole de chiffrement qui vous est adéquat afin d'échanger plus facilement avec vos partenaires (AS2, AS3, AS4, OpenPGP, ZIP avec AES, SFTP, FTPS ou HTTPS).

Les solutions de transferts de fichiers (MFT) s'intègrent aisément au cloud et aux applications. Elles gèrent les clés et les certificats, suivent toute l'activité des transferts de fichiers, respectent les réglementations strictes, etc.

Ce sont bien évidemment vos besoins professionnels qui vous aideront à déterminer la méthode la plus adaptée à vos exigences en matière de sécurité.

11. Comment choisir la bonne méthode de chiffrement pour votre entreprise ?

A. Les questions essentielles à se poser

Plusieurs facteurs sont à prendre en compte lorsque vous souhaitez implémenter un protocole de chiffrement. Voici quelques questions essentielles à ne pas oublier de vous poser :

- **Mes données échangées sont-elles sensibles ?**

Quels types de données est-ce que j'échange au quotidien avec mes partenaires et clients ?

Chaque entreprise doit protéger les données qu'elle collecte, stocke et partage (RGPD). Beaucoup choisissent un logiciel de chiffrement de fichiers qui est l'un des moyens les plus simples de protéger vos données aussi bien au repos, qu'en mouvement.

- **Comment seront transmises mes informations ?**

Transportez-vous des fichiers par FTP, courrier électronique, HTTP ou une autre méthode ? Êtes-vous en mesure de chiffrer les données selon les besoins ?

Faciliter la circulation des données en toute sécurité est l'un des besoins primaires. Si vous transférez des données confidentielles et volumineuses, assurez-vous que le logiciel peut gérer correctement ces échanges.

- **Répond-il à mes exigences réglementaires ?**

Les entreprises ont souvent le choix parmi une multitude de normes de chiffrement. Cependant, les réglementations et exigences spécifiques orientent souvent vers certains types de chiffrement des données plutôt que d'autres. Vérifiez bien l'adéquation du logiciel de chiffrement avec les normes de conformité exigées dans votre entreprise.

- **Est-il compatible avec ma plateforme système ?**

La plupart des outils de chiffrement de fichiers fonctionnent sur les plateformes les plus populaires, que ce soit sur site ou dans le cloud. Assurez-vous que votre logiciel de chiffrement est bien compatible avec vos systèmes, applications et ceux de vos partenaires.

B. Les protocoles recommandés selon votre besoin

Exemple 1 : données peu sensibles mais protection par mot de passe requis.

Vous devez envoyer votre liste de prix à vos clients par courrier électronique.Vous voulez qu'il soit facile pour les clients d'ouvrir le fichier. Bien que les informations de cette liste de prix ne soient pas extrêmement sensibles, vous souhaitez au moins les protéger par un mot de passe.

Recommandation : ZIP avec chiffrement AES

Exemple 2 : données bancaires sensibles et connexion SFTP.

Vous devez transmettre à la banque les informations relatives au dépôt direct de votre entreprise. Il s'agit d'informations très sensibles. Votre banque veut éviter de transmettre ces informations sensibles et souhaite renforcer la sécurité lors du transfert de ce fichier.

Recommandation : chiffrement PGP/GPG

Exemple 3 : authentification par mot de passe ou clé publique avec connexion FTP.

Votre partenaire commercial souhaite échanger des informations avec vous via une connexion FTP sécurisée. Ce partenaire commercial souhaite authentifier votre entreprise avec un mot de passe ou une clé publique.

Recommandation : SFTP

Exemple 4 : fichiers volumineux et sensibles par FTP ou email.

Vous devez envoyer des commandes à vos fournisseurs, dont les données sont considérées comme assez sensibles. Les fichiers peuvent être assez volumineux et doivent être compressés avant d'être envoyés. Les commandes doivent être envoyées par des connexions FTP standards ou par courrier électronique.

Recommandation : Zip avec chiffrement

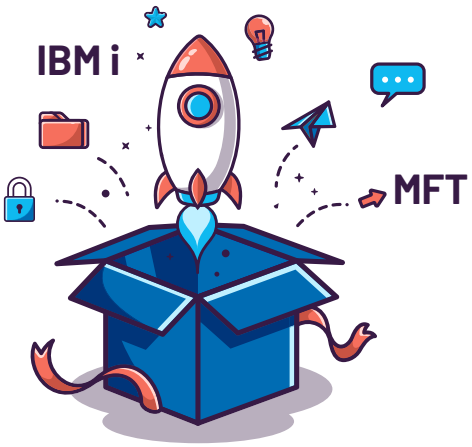
12. Conclusion

Le chiffrement est donc une technologie phare de la cybersécurité. Elle est recommandée aussi bien par les organismes mondiaux, que les réglementations. Si celle-ci ne cesse d'évoluer dans le monde technologique, elle n'en reste pas moins un processus ancestral. Ce pilier de l'informatique est incontournable dans bon nombre de logiciels vendus aujourd'hui.

13. Tips solutions

A. Chiffrement IBM i

Powertech Encryption est une solution de chiffrement solide et performante pour système . Rapide à implémenter, la solution chiffre les données applicatives et les sauvegardes.
Elle répond favorablement aux contraintes réglementaires telles que Bâle3, HIPAA, SOX, etc.



Powertech Encryption utilise les algorithmes de chiffrement éprouvés AES et TDES.

Découvrez les autres atouts d'audit et de tokenisation de Powertech Encryption autour d'une démo.

B. Transferts de fichiers sécurisés

GoAnywhere MFT est une solution de transferts de fichiers gérés.

La solution automatise le processus de chiffrement et de déchiffrement afin de garantir la sécurité des fichiers. Flexible, vous pouvez choisir la norme de chiffrement requise par votre entreprise.

GoAnywhere MFT s'intègre en toute sécurité au cloud et aux applications, gère les clés et les certificats, suit toute l'activité de transfert de fichiers, respecte les réglementations, etc.

La solution fonctionne sur la plupart des environnements techniques. Découvrez toutes les possibilités de transferts sécurisés autour d'une démonstration ou d'un

Agence commerciale France

Tel : +33 9 70 75 61 13
Email : sales@bluefinch-esbd.com
Adresse : 14 rue du Pré Paillard
Parc des Glaisins
74940 Annecy-le-Vieux, France