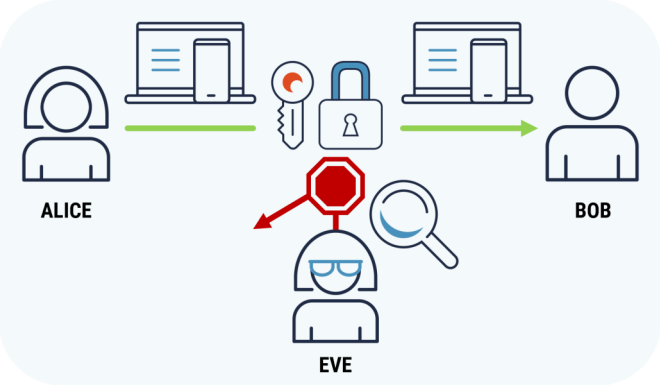
UTILISER LE CHIFFREMENT POUR ASSURER LA SÉCURITÉ DES DONNÉES SENSIBLES

MAI 2021 ITSAP.40.016

Les technologies de chiffrement servent à sécuriser nombre d'applications et de sites Web que vous consultez tous les jours, comme les services bancaires et les achats en ligne, les applications de messagerie électronique et la messagerie instantanée sécurisée. Elles assurent la sécurité de l'information lorsqu'elle est en transit (p. ex. au moment de se connecter à un site Web) et inactive (p. ex. stockée dans des bases de données chiffrées). Le chiffrement est intégré à bon nombre des plus récents systèmes d'exploitation, dispositifs mobiles et services d'infonuagique, mais en quoi cela consiste-t-il exactement? Comment l'utilise-t-on? Quels facteurs votre organisation devrait-elle prendre en considération avant de l'utiliser?

QU'EST-CE QUE LE CHIFFREMENT?

Le chiffrement est un mécanisme qui consiste à coder (ou brouiller) l'information. Le chiffrement protège la confidentialité de l'information en empêchant les personnes non autorisées d'y accéder.



Par exemple, Alice veut envoyer un message à Bob et s'assurer que personne d'autre ne puisse le lire. Elle chiffre le message au moyen d'une clé secrète pour veiller à ce que l'information demeure confidentielle et privée. Une fois chiffré, le message ne peut être lu que par le détenteur de la clé secrète nécessaire au déchiffrement. Dans ce cas-ci, Bob possède la clé secrète.

Ève tente délibérément d'intercepter le message et de le lire. Par contre, même si elle obtient une copie du message, elle ne pourra pas le lire sans obtenir la clé secrète parce qu'il est chiffré.

Si une personne reçoit par accident un message qui contient de l'information chiffrée, elle ne pourra pas lire le message sans la clé nécessaire au déchiffrement.

COMMENT UTILISE-T-ON LE CHIFFREMENT?

Le chiffrement est une partie importante de la cybersécurité. On l'utilise de maintes façons pour veiller à ce que les données soient confidentielles et privées. C'est le cas, entre autres, sur les sites Web HTTPS, dans les applications de messagerie sécurisée, dans les services de courriel et sur les réseaux privés virtuels. Le chiffrement permet de protéger l'information alors qu'elle se déplace d'un endroit à l'autre (c.-à-d., lorsqu'elle est en transit), entre l'expéditeur et le destinataire. Par exemple, lorsque vous vous connectez au site Web de votre institution financière au moyen de votre portable ou de votre téléphone cellulaire, les données qui sont transmises entre votre dispositif et le site Web en question sont chiffrées. Le chiffrement sert également à protéger les données inactives. On ne peut, par exemple, lire le format des données stockées dans les bases de données chiffrées. Même si un auteur de menace arrive à accéder à la base de données, une couche de sécurité additionnelle l'empêchera d'accéder à l'information qu'elle contient. Le chiffrement sert également à protéger les renseignements personnels que vous transmettez aux organisations. Si vous fournissez des renseignements personnels (p. ex. une date de naissance, des données bancaires ou de l'information sur une carte de crédit) à un détaillant en ligne, assurez-vous de protéger ces renseignements par chiffrement en faisant appel à la navigation sécurisée.

Plusieurs fournisseurs de services d'infonuagique ont recours au chiffrement pour protéger vos données lorsque vous utilisez leurs services en nuage. Ces services offrent la possibilité de conserver le chiffrement des données lors du téléversement ou du téléchargement de fichiers et de stocker des données chiffrées pour les protéger lorsqu'elles sont inactives.

S'il est mis en œuvre correctement, le chiffrement est un mécanisme que votre organisation et vous pouvez utiliser pour assurer la confidentialité de vos données. L'intégration du chiffrement s'effectue sans problème dans de nombreuses applications pour permettre aux utilisateurs de les employer en toute sécurité.

SÉRIE SENSIBILISATION

No de cat. D97-1/40-016-2021F-PDF
ISBN 978-0-660-38619-5

COMMENT PUIS-JE UTILISER LE CHIFFREMENT?

Votre organisation utilise probablement déjà le chiffrement à plusieurs fins, comme la navigation sécurisée et les applications de messagerie chiffrée.

NAVIGATION SÉCURISÉE

Si vous accédez à un site Web affichant une icône en forme de cadenas et dont l'adresse commence par HTTPS, vous savez que celui-ci chiffrera la communication (c.-à-d. les données échangées entre votre dispositif et les serveurs du site Web).

Pour protéger l'information et les systèmes de votre organisation, on recommande d'utiliser les adresses HTTPS dans la mesure du possible. Pour veiller à ce que les utilisateurs accèdent uniquement aux sites Web pris en charge par le protocole HTTPS, votre organisation devrait mettre en œuvre l'outil de stratégies de sécurité Web du protocole HSTS (HTTP Strict Transport Security). Le protocole HSTS offre une sécurité additionnelle, puisqu'il force les navigateurs à charger des sites Web prenant en charge le protocole HTTPS et à ignorer les sites Web non sécurisés (p. ex. HTTP).

APPLICATIONS DE MESSAGERIE CHIFFRÉE

La plupart des applications de messagerie instantanée offrent une certaine protection par chiffrement pour assurer la confidentialité de votre information. Dans certains cas, les messages sont chiffrés entre votre dispositif et le stockage en nuage utilisé par le fournisseur du service de messagerie. Dans d'autres, les messages sont chiffrés à partir de votre dispositif jusqu'à celui du destinataire (c.-à-d., chiffrement de bout en bout). Avec le chiffrement de bout en bout, personne ne peut lire vos messages chiffrés, pas même le fournisseur du service de messagerie.

Au moment de choisir vos outils, vous devez tenir compte de la fonctionnalité du service, ainsi que des exigences en matière de sécurité et de confidentialité auxquelles sont assujetties votre information et de vos activités. Pour obtenir de plus amples informations à ce sujet, veuillez consulter le document *Protégez-vous en ligne*.

Le chiffrement n'est qu'un des nombreux contrôles de sécurité nécessaires pour protéger la confidentialité des données.

QUELS AUTRES FACTEURS DEVRAIS-JE PRENDRE EN CONSIDÉRATION?

Le chiffrement s'intègre à de nombreux produits utilisés dans le cadre d'activités quotidiennes. Si vous optez pour un produit faisant appel au chiffrement, il est recommandé de choisir un produit certifié selon les Critères communs (CC) et dans le cadre du Programme de validation des modules cryptographiques (PVMC). Les CC et le PVMC dressent la liste des modules cryptographiques qui sont conformes aux normes FIPS (Federal Information Processing Standards). Les CC et le PVMC servent à approuver les produits utilisés par le gouvernement fédéral, mais il est recommandé à tous d'utiliser ces produits certifiés.

RECOMMANDATIONS DU CCC

Pour choisir un produit de chiffrement qui répond aux besoins votre organisation :

- évaluez la sensibilité de votre information (p. ex. données personnelles et exclusives) afin de déterminer dans quelle mesure elle peut être à risque, puis mettre en œuvre le chiffrement en conséquence;
- choisissez un fournisseur qui a recours à des algorithmes de chiffrement normalisés (p. ex. modules validés selon les CC et le PVMC);
- passez en revue votre plan de gestion du cycle de vie de produits TI et votre budget de manière à tenir compte des mises à jour logicielles et matérielles relatives à vos produits de chiffrement;
- appliquez fréquemment les mises à jour et les correctifs sur vos systèmes.

  L'informatique quantique sera bientôt une menace pour la cybersécurité. Préparez-vous en conséquence. Pour obtenir de plus amples informations à ce sujet, consultez le document *ITSE.00.017 Faire face à la menace que l'informatique quantique fait peser sur la cryptographie*.

LE CHIFFREMENT DES DONNÉES TRÈS SENSIBLES

Il convient d'appliquer des mesures de sécurité additionnelles aux systèmes qui contiennent de l'information très sensible (p. ex. les établissements financiers, médicaux et gouvernementaux). Pour obtenir d'autres conseils relatifs aux solutions cryptographiques pour les systèmes et l'information très sensibles, communiquez avec nous par courriel à l'adresse suivante : **contact@cyber.gc.ca**

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.