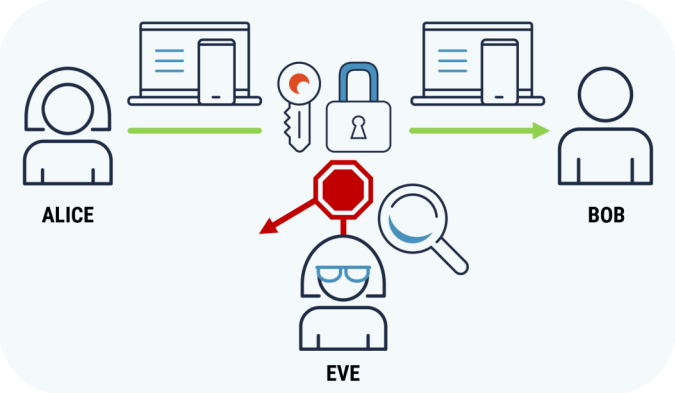
UTILISER LE CHIFFREMENT POUR ASSURER LA SÉCURITÉ DES DONNÉES SENSIBLES

OCTOBRE 2020 **ITSAP.40.016**

Les technologies de chiffrement servent à sécuriser plusieurs des applications et des sites Web que vous utilisez 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). 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 à 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 peut être lu par quiconque possède la clé secrète nécessaire au déchiffrement. Dans ce cas-ci, Bob possède la clé secrète.

Ève, une cybercriminelle, tente d'intercepter le message et de le lire. Par contre, même si elle arrive à le copier, elle ne pourra lire le message sans obtenir la clé secrète, puisque celui-ci est chiffré.

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 d'hébergement de courrier et sur les réseaux privés virtuels. Le chiffrement permet de protéger l'information alors qu'elle se déplace d'un emplacement 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. 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, vous devez vous assurer de protéger ces renseignements par chiffrement en faisant appel à la navigation sécurisée.

Plusieurs fournisseurs de services d'infonuagique ont également recours au chiffrement pour protéger vos données lorsque vous utilisez leurs services en nuage. Les données sont chiffrées au moment où vous téléversez ou téléchargez des fichiers par l'entremise de ces services.

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 plusieurs applications pour permettre aux utilisateurs d'en faire l'emploi en toute sécurité.

SÉRIE SENSIBILISATION

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 arborant une icône en forme de cadenas et dont l'adresse commence par HTTPS (tel qu'il est illustré dans l'image ci-dessous), 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 un niveau de chiffrement suffisant pour protéger 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). L'utilisation de services de chiffrement de bout en bout fait en sorte que même le fournisseur du service de messagerie ne peut lire vos messages chiffrés.

Au moment de décider des outils qu'il convient d'utiliser, vous devez tenir compte de la fonctionnalité du service, ainsi que des exigences en matière de sécurité et de confidentialité de votre information et de vos activités.

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 plusieurs produits souvent utilisés par les utilisateurs et les organisations dans le cadre de leurs 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 Standard*). Comme les CC et le PVMC sont utilisés par le gouvernement fédéral pour approuver l'utilisation de produits, il est recommandé à tous d'utiliser ces produits certifiés.

CHIFFREMENT DES SYSTÈMES ET DE L'INFORMATION À SENSIBILITÉ ÉLEVÉE

Les systèmes et l'information à sensibilité élevée exigent des considérations de sécurité additionnelles. Pour choisir un produit adéquat, considérez les points suivants :

- 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 ayant fait l'objet d'une validation (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;
- appliquer fréquemment les mises à jour et les correctifs sur vos systèmes.

Si votre organisation gère de l'information et des systèmes de nature très sensible, vous devriez envisager de prendre les mesures nécessaires pour atténuer la menace que pose l'informatique quantique sur la cybersécurité. Prière de consulter l'ITSE.00.017, *Enjeux de sécurité de l'informatique quantique pour la cryptographie à clé publique*.

Pour de plus amples conseils sur les solutions cryptographiques pour les systèmes et l'information à sensibilité élevée, communiquez avec nous par courriel à **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**.