PRÉPAREZ VOTRE ORGANISATION À LA MENACE QUE POSE L'INFORMATIQUE QUANTIQUE POUR LA CRYPTOGRAPHIE

FÉVRIER 2021

ITSAP.00.017

Avoir recours à la cryptographie est un moyen efficace d'assurer la confidentialité et l'intégrité de l'information et de protéger les systèmes de TI contre les auteurs de cybermenace. L'informatique quantique menace de craquer la plupart des mécanismes cryptographiques que nous employons actuellement. Les ordinateurs quantiques utiliseront la physique quantique pour traiter l'information avec efficience et résoudront des problèmes qu'il est difficile de résoudre au moyen des capacités de traitement actuelles. Les ordinateurs quantiques n'ont pas la puissance nécessaire pour venir à bout des techniques de cryptographie, mais un auteur de menace pourrait un jour disposer d'un ordinateur quantique suffisamment puissant pour déchiffrer, lire ou consulter l'information sensible.

EN QUOI VOTRE CYBERSÉCURITÉ EST-ELLE TOUCHÉE?

Les progrès réalisés dans le domaine de l'informatique quantique mettent à risque la cybersécurité de votre organisation. Bien que les ordinateurs quantiques actuels n'aient pas la puissance nécessaire pour venir à bout des techniques de cryptographie, un ordinateur suffisamment puissant pourrait être disponible d'ici 2030.

La cryptographie protège l'information et les systèmes de TI en faisant appel au chiffrement, à l'intégrité et à l'authentification.

Le chiffrement est utilisé pour protéger la confidentialité de l'information stockée sur un dispositif (p. ex. un téléphone intelligent, des clés USB) ou transmise à partir de ce dernier.

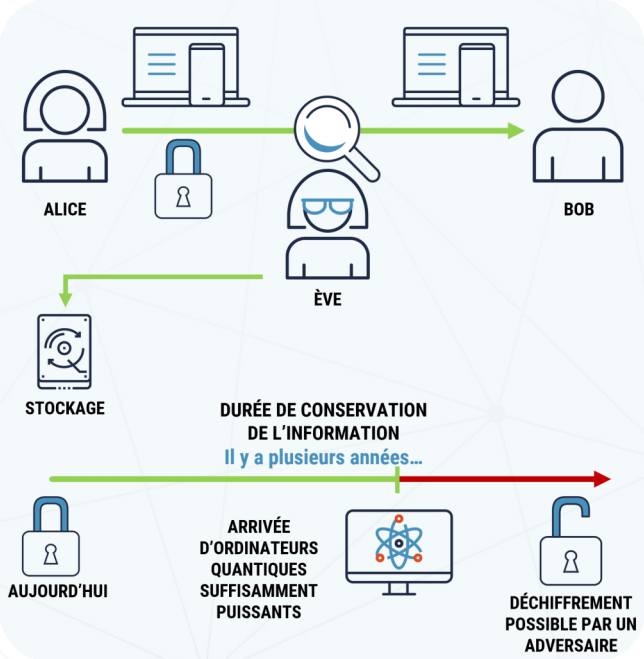
Les auteurs de menace peuvent stocker l'information chiffrée afin de la déchiffrer plus tard, à l'arrivée d'ordinateurs quantiques suffisamment puissants. Ces derniers pourraient être en mesure de déchiffrer de l'information ayant une durée de conservation moyenne ou longue (c.-à-d., qu'il faudra toujours protéger dans 10 ans ou plus).

Par durée de conservation, on entend la durée pendant laquelle il est nécessaire de protéger l'information détenue par votre organisation (p. ex. garantir la confidentialité et protéger la propriété intellectuelle).

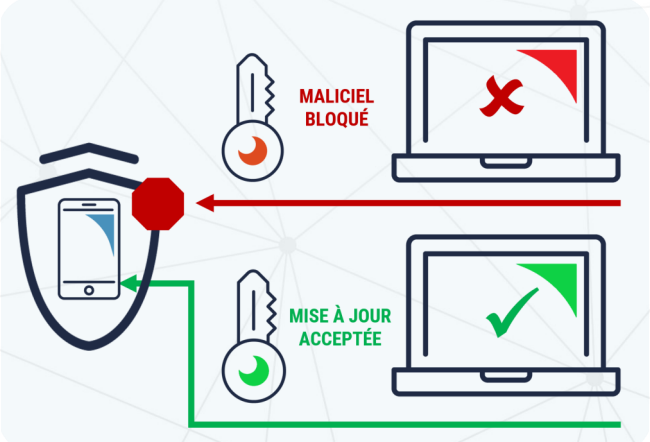
L'intégrité et l'authentification permettent de veiller à ce que l'information ne soit pas modifiée accidentellement ou intentionnellement lorsqu'elle est en transit ou en stockage, et qu'elle provient de la source appropriée.

Des auteurs de menace pourraient utiliser un ordinateur quantique suffisamment puissant pour se faire passer pour des systèmes de confiance (p. ex. une boutique d'applications ou un fournisseur de confiance) afin de fournir de fausses mises à jour logicielles et d'accéder aux systèmes d'intérêt. Contrairement à la confidentialité, l'intégrité et l'authentification ne seront à risque qu'après l'arrivée d'ordinateurs quantiques suffisamment puissants.

UN AUTEUR DE MENACE STOCKE DES DONNÉES CHIFFRÉES POUR LES DÉCHIFFRER ULTÉRIEUREMENT :



UN AUTEUR DE MENACE ENVOIE DE FAUSSES MISES À JOUR LOGICIELLES POUR ACCÉDER AUX SYSTÈMES :



SÉRIE SENSIBILISATION

EN QUOI VOS SYSTÈMES DE TI SONT-ILS TOUCHÉS?

L'information ayant une durée de conservation moyenne ou longue qui est stockée dans vos systèmes de TI pourrait être à risque. Bien que les systèmes utilisés pour procéder à l'authentification et assurer l'intégrité des données ne soient pas à risque aujourd'hui, ils pourraient être la cible d'un auteur de menace.

Votre organisation devrait mettre en place un plan de transition et allouer les budgets nécessaires pour mettre à niveau les systèmes de TI, et déployer des mécanismes de cryptographie post-quantique normalisés lorsque cette technologie sera disponible. Les praticiens devraient demander aux fournisseurs s'ils envisagent de procéder à une mise à niveau sécurisée de leur matériel et de leurs logiciels afin d'y intégrer des mécanismes de cryptographie post-quantique. Dans le cadre de cette transition, des mises à jour logicielles et des correctifs devraient être appliqués aux systèmes au moyen du chiffrement pour assurer la sécurité de la mise à niveau et authentifier la source.

L'élaboration de ce plan devrait accorder la priorité à l'information sensible ayant une durée de conservation longue (p. ex. la propriété intellectuelle, les données fiscales, les dossiers médicaux).

EXISTE-T-IL UNE SOLUTION QUANTIQUE?

Une future technologie quantique et la distribution quantique de clés (DQC) pourraient également être utilisées pour protéger l'information sensible. Malgré les progrès réalisés sur le plan de la sécurité et de l'adaptabilité de la DQC, son développement n'a pas encore atteint tout son potentiel. La DQC n'a pas pour objet de remplacer les applications de chiffrement actuelles, mais elle pourrait offrir une façon sécurisée de communiquer dans un avenir prochain.

QUE FAIT LE CENTRE CANADIEN POUR LA CYBERSÉCURITÉ ?

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) s'efforce de sensibiliser le public et les organisations aux menaces que posent les ordinateurs quantiques sur le plan du chiffrement et aux étapes qu'il leur faudra suivre pour se préparer à l'arrivée de la cryptographie post-quantique.

Le Centre pour la cybersécurité collabore avec le National Institute for Standards in Technology[1] (NIST) et d'autres partenaires à l'évaluation de la nouvelle génération de mécanismes de cryptographie post-quantique en vue de remplacer les applications de chiffrement actuelles.

Le Centre pour la cybersécurité participe activement aux activités de normalisation internationale, dont celles menées par l'Organisation internationale de normalisation (ISO pour *International Standards Organization*) et de l'Internet Engineering Task Force, pour veiller à ce que la sécurité cryptographique et les besoins des Canadiens en matière de vie privée soient pris en compte dans les nouvelles normes imposées par la cryptographie post-quantique.

COMMENT LES ORGANISATIONS PEUVENT-ELLES GÉRER LES RISQUES?

On recommande à votre organisation de prendre les mesures suivantes pour aider à pallier les risques liés aux progrès réalisés dans le domaine de l'informatique quantique et de planifier sa transition à la cryptographie post-quantique :

1. Évaluez le niveau de sensibilité et la durée de conservation de l'information de votre organisation afin de déterminer les risques qui pourraient peser sur celle-ci (p. ex. un élément des processus d'évaluation continue des risques).
2. Passez en revue votre gestion du cycle de vie des produits TI et mettez en place un plan pour faciliter l'adoption de la cryptographie post-quantique dès son arrivée.
3. Prévoyez un budget pour des mises à jour matérielles et logicielles potentiellement considérables lorsque viendra le temps de procéder aux remplacements nécessaires.
4. Assurez-vous que vos équipes et vous êtes au courant des nouvelles menaces et des futures technologies quantiques.
5. Demandez à vos fournisseurs s'ils planifient de mettre en place des mécanismes de cryptographie post-quantique (p. ex. les fournisseurs envisagent-ils d'intégrer la cryptographie post-quantique à de futures mises à jour ou devrez-vous vous procurer du nouveau matériel et de nouveaux logiciels?).
6. Assurez-vous que votre fournisseur a recours à des mécanismes cryptographiques normalisés et validés (p. ex. Federal Information Processing Standards [FIPS]).
7. Déterminez à quel moment et de quelle façon vous intégrerez les algorithmes post-quantiques à votre plan de gestion du cycle de vie.
8. Appliquez fréquemment les mises à jour et les correctifs sur les systèmes.

Communiquez avec le Centre pour la cybersécurité) par courriel à contact@cyber.gc.ca ou par téléphone au 1-888-CYBER-88 pour de plus amples recommandations.

RÉFÉRENCES :

Le Centre pour la cybersécurité et le NIST[1] : *Post-Quantum Cryptography*. février 2020.

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**.