FAIRE FACE À LA MENACE QUE L'INFORMATIQUE QUANTIQUE FAIT PESER SUR LA CRYPTOGRAPHIE

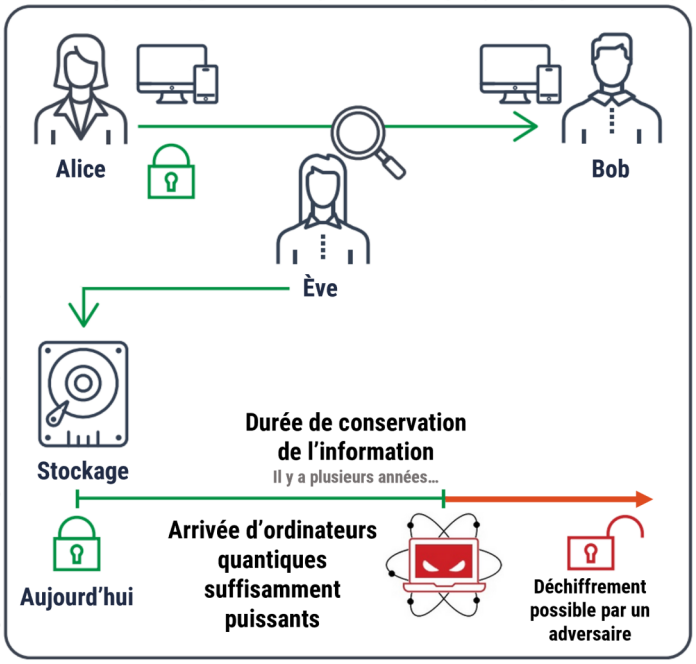
MAI 2020 ITSE.00.017

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 arriveront à solutionner des problèmes qu'il est difficile de résoudre au moyen des capacités de traitement actuelles. Les ordinateurs que l'on peut acheter aujourd'hui n'ont pas la puissance nécessaire pour venir à bout des techniques de cryptographie, mais la technologie évolue rapidement et pourrait être accessible d'ici 2030. Dans un jour prochain, un auteur de menace pourrait disposer d'un ordinateur quantique suffisamment puissant pour déchiffrer, lire ou consulter l'information sensible, et ce, bien après qu'elle a été créée.

DURÉE DE CONSERVATION DE L'INFORMATION

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

Les auteurs de menace peuvent stocker l'information chiffrée indéfiniment afin de la déchiffrer plus tard, à l'arrivée d'ordinateurs quantiques suffisamment puissants. Ceux-ci pourraient donc 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).



Ève peut obtenir et stocker dès maintenant de l'information ayant une durée de conservation moyenne ou longue afin de la déchiffrer à l'arrivée d'ordinateurs quantiques suffisamment puissants.

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**.

FUTURE TECHNOLOGIE

Une future technologie quantique pourrait également être utilisée pour protéger l'information sensible. La distribution quantique de clés (DQC) en est un exemple. Malgré les progrès réalisés sur le plan de la faisabilité et 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 pourrait offrir une façon sécurisée de transmettre les clés dans un avenir prochain.

Le Centre canadien pour la cybersécurité collabore avec le NIST[1] et d'autres partenaires au développement de la nouvelle génération de mécanismes de cryptographie post-quantique pour les ordinateurs traditionnels (p. ex. en vue de remplacer les applications de chiffrement actuelles). L'intégration de ces nouveaux composants exigera la mise à jour logicielle et matérielle des systèmes de TI existants, ce qui pourrait nécessiter des investissements considérables.

GESTION DES RISQUES

Pour gérer les risques associés aux progrès réalisés sur le plan de l'informatique quantique, on recommande de suivre les trois étapes suivantes :

1. Évaluer le niveau de sensibilité et la durée de conservation de l'information de l'organisation afin de déterminer les risques qui pourraient peser sur celle-ci (p. ex. une partie des processus d'évaluation continue des risques);
2. Passer en revue le plan de gestion du cycle de vie de produits TI et le budget de l'organisation pour relever les éventuelles mises à jour logicielles et matérielles importantes;
3. Sensibiliser le personnel aux enjeux de la menace quantique.

Communiquez avec le Centre canadien pour la cybersécurité (contact@cyber.gc.ca ou 1-888-CYBER-88) pour obtenir de plus amples renseignements et conseils.

RÉFÉRENCES :

Centre canadien pour la cybersécurité et NIST[1] : *Post-Quantum Cryptography* (en anglais seulement)

SÉRIE HAUT DIRIGEANTS