Ministère
de l'Éducation
et de l'Enseignement
supérieur
Québec

Rapport COCD MÉES sur la sécurité de l'application Zoom

La plateforme de vidéoconférence Zoom est riche en fonctionnalités et comporte une multitude d'outils pour améliorer la confidentialité et la sécurité d'une réunion en mode vidéo. Durant la période de confinement à l'échelle planétaire, le besoin des utilisateurs en conférences à distance a augmenté et la plateforme a vu son nombre d'utilisateurs grandir de manière exponentielle. Dès lors, les professionnels en cybersécurité ont concentré leurs activités sur le sujet et mis en lumière plusieurs failles de sécurité de cette solution.

Engagement de l'éditeur :

Malgré la multiplication des vulnérabilités découvertes sur la solution Zoom, le support de la compagnie s'est montré très réactif. En effet, la société a orienté ses équipes vers la correction des problèmes au lieu de développer de nouvelles fonctionnalités. Le résultat de cette politique s'est répercuté sur leur réactivité accrue face aux différents incidents et vulnérabilités détectés et plusieurs correctifs de sécurité ont été publiés. Cela dit, afin de bénéficier des fonctionnalités offertes par la solution tout en restant sécurisé, il est recommandé d'utiliser la dernière version logicielle disponible sur le portail de l'éditeur « https://zoom.us/download » pour chaque réunion.

Fausses alertes :

Dernièrement, un des principaux évènements médiatiques entourant la plateforme relate la vente de plus 500 000 comptes Zoom sur le web caché (« dark web ») et sur les forums des « hackers ». L'information a révélé que plusieurs de ces comptes étaient associés à des établissements scolaires et à des banques. Il est important de préciser qu'il ne s'agit pas de fuite de données au niveau de la plateforme de vidéoconférence Zoom, mais bien de « credential stuffing », un type de cyberattaque qui consiste à obtenir l'accès à un compte en se servant de mots de passe trouvés grâce à d'autres attaques ou fuites de données qui ne sont pas forcément liés à Zoom. Une étude réalisée par Google démontre que 1,5 % des internautes utilisent des mots de passe déjà piratés1. Les utilisateurs sont eux aussi responsables de la sécurité de leurs comptes.

Configuration particulière pour améliorer la sécurité de Zoom :

Afin d'améliorer la protection des informations échangées sur la plateforme de vidéoconférence, il convient d'appliquer la configuration suivante :

Activer :

- Activation de la salle d'attente (waiting room);
- Activer la fonctionnalité « Uniquement les utilisateurs authentifiés peuvent rejoindre les réunions ».

Désactiver :

- Désactivation de l'accès à la réunion avant l'arrivée de l'animateur;
- Désactiver la fonction « Permettre aux participants de se renommer » (Allow participants to rename themselves);
- Désactiver la fonction « intégrez le mot de passe dans le lien de la réunion pour rejoindre en un clic »;
- Désactiver la fonction de partage de fichiers entre les participants;
- Désactivation de l'enregistrement des rencontres par les participants;
- Spécifier qui peut partager son écran.

Bonnes pratiques de sécurité globale :

Utiliser les dernières versions disponibles pour tous les logiciels et plus particulièrement pour le système d'exploitation, l'antivirus, la suite bureautique et le navigateur web.

Changer régulièrement vos mots de passe, peu importe la plateforme, et utiliser des mots de passe différents pour chacun de vos comptes. L'utilisation d'un gestionnaire de mots de passe comme « KeePass », « LastPass » ou autre peut s'avérer utile. Ils permettent une gestion facile et simple de tous vos mots de passe sans les enregistrer sur son navigateur web. Ils permettent également de créer des mots de passe complexes et ultra-sécurisés sans avoir besoin de s'en souvenir.

Éviter de partager une information confidentielle sur les plateformes similaires à Zoom, Hangout ou Skype. Il est préférable d'utiliser des outils fournis par votre organisation.

[1] https://research.google/pubs/pub48399/