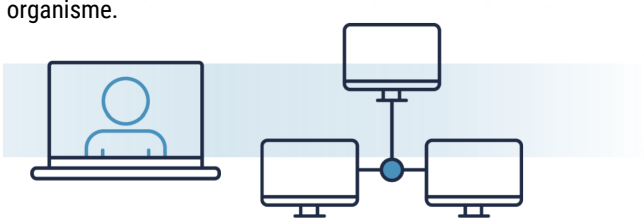
VIDÉOCONFÉRENCE

MAI 2020

ITSAP.10.216

Grâce au recours à la vidéoconférence, votre organisation peut organiser des rencontres et travailler avec les employés, les clients et les partenaires qui se trouvent dans divers emplacements géographiques. Toutefois, la vidéoconférence comporte des risques sur le plan de la sécurité et de la protection de la vie privée, et ces risques doivent être pris en compte avant de choisir, d'installer et d'utiliser ces applications au sein de votre organisme. Il conviendra donc d'établir la liste des menaces et des risques liés à ces outils, ce qui vous permettra de mettre en œuvre les mesures de sécurité appropriées ainsi que les pratiques exemplaires visant à protéger l'environnement de travail virtuel de votre organisme.



AVANTAGES

Les applications de vidéoconférence peuvent accroître la productivité et le degré de collaboration entre les employés, les clients et les partenaires. Ces applications sont plus conviviales que les appels téléphoniques, puisqu'elles ont l'avantage d'offrir une interaction en face à face entre les participants. Nombre d'entre elles disposent d'outils de collaboration intégrés (par exemple, le partage des contenus d'écran et des fichiers ou la possibilité d'enregistrer les réunions) et permettent d'organiser des rencontres pour des groupes de diverses tailles, sans les contraintes normalement liées à l'espace physique.

De nombreuses applications sont disponibles gratuitement ou sont offertes selon des options d'abonnement tarifées en fonction d'une grille de prix dégressive pour s'adapter aux besoins de votre organisme.

RISQUES

Bon nombre d'applications de vidéoconférence sont offertes dans le marché. Or, l'accent que le fournisseur met sur la sécurité, et la façon dont vous utiliserez et sécuriserez ces applications auront une influence sur la sécurité des systèmes et des informations de votre organisme.

En outre, les auteurs malveillants peuvent tenter d'exploiter les vulnérabilités et les failles des logiciels en lançant des attaques en force dans le but de subtiliser des renseignements ou d'accéder à des discussions privées.

Lorsque des informations sensibles sont transmises ou échangées en cours de réunion par vidéoconférence, il y a un risque accru de violation de la confidentialité des données ou des renseignements personnels, ce qui peut porter atteinte à la réputation de votre organisme et à ses relations avec ses clients et partenaires.

MENACES

Les auteurs malveillants ciblent les applications de vidéoconférence afin de perturber les réunions, de surcharger les services, d'écouter les appels et de subtiliser des informations. Au reste, ces auteurs malveillants utilisent différentes méthodes pour s'attaquer aux applications de vidéoconférence :

- **Attaques en force** : Un auteur malveillant balaie automatiquement une liste d'identifiants de réunion pour tenter de se connecter au système de vidéoconférence.
- **Sabotage de réunion** (*meeting bombing*) : Un auteur malveillant se joint à une réunion pour écouter les conversations ou perturber la réunion en partageant un contenu inapproprié ou explicite.
- **Grattage d'écran** : Un auteur malveillant collecte des données affichées à l'écran d'un système compromis.
- **Maliciel** : Un auteur malveillant tente d'infecter des dispositifs en partageant des pièces jointes, des applications ou des liens pouvant mener à des hôtes malveillants (p. ex. des sites Web, des logiciels).
- **Hameçonnage** : Un auteur malveillant peut tenter d'organiser une vidéoconférence en imitant un contact digne de confiance (p. ex. avec une caméra qui ne fonctionne pas).
- **Menace interne** : Le personnel d'un fournisseur d'application de vidéoconférence peut accidentellement ou délibérément compromettre les réunions de votre organisme. Par exemple, un employé n'ayant pas reçu la formation appropriée peut partager par erreur des informations confidentielles (p. ex. les justificatifs d'accès aux réunions).

Ne partagez jamais d'information sensible par l'intermédiaire d'applications de vidéoconférence. Utilisez plutôt d'autres méthodes lorsque vous devez partager des informations sensibles (p. ex. un système de messagerie sécurisée par chiffrement).

ADOPTER DES PRATIQUES SÉCURITAIRES

Pour atténuer les risques associés à l'utilisation des applications de vidéoconférence, votre organisme doit prendre des précautions au moment de choisir, d'installer et d'utiliser une application. En l'occurrence, il convient de prendre en compte les conseils suivants.

CHOISIR UNE APPLICATION

- Téléchargez les applications offertes par des fournisseurs fiables.
- Utilisez les solutions organisationnelles existantes dans la mesure du possible.
- Utilisez une application de vidéoconférence dotée de contrôles de sécurité qui peuvent être personnalisés pour répondre à vos besoins (p. ex. les contrôles de sécurité peuvent différer entre les versions gratuites et les versions payantes de l'application).
- Faites appel à des fournisseurs qui respectent les lois canadiennes sur la protection de la vie privée, pour veiller à ce que vos informations soient protégées contre les utilisateurs non autorisés et les partages interdits.
- Testez l'application avant de l'utiliser au sein de votre organisation.

SÉCURISER L'APPLICATION

- Tenez les applications à jour ou envisagez d'utiliser une solution qui ne nécessite pas l'installation de logiciels par les participants, sauf lorsque c'est nécessaire (p. ex. les versions Web des applications de vidéoconférence ne requièrent aucune mise à jour de la part des utilisateurs).
- Modifier les paramètres par défaut, car ils sont souvent moins sûrs.
- Désactivez les fonctions dont vous n'avez pas besoin (p. ex. l'échange de fichiers, le partage d'écran, le générateur de transcriptions).
- Veillez à ce que les privilèges administratifs soient réservés aux personnes autorisées.

SÉCURISER LES RÉUNIONS

- Sécurisez les réunions au moyen d'une phrase de passe ou d'un mot de passe.
- Gardez confidentiels l'hyperlien et le mot de passe des réunions.
- Assurez-vous que les participants ne peuvent se joindre à la réunion que si l'hôte est présent.
- Utilisez une salle d'attente pour les participants, s'il y en a une qui est disponible.
- Réduisez au minimum le nombre d'administrateurs ou d'hôtes d'une réunion.
- Ne transmettez jamais d'information sensible par l'intermédiaire d'applications de vidéoconférence.

INTERVENIR EN CAS D'INCIDENT

Dès que vous soupçonnez que vos vidéoconférences ont été la cible d'activités malveillantes :

1. Arrêtez la réunion;
2. Repérez l'information qui est à risque (c.-à-d. l'information opérationnelle ou personnelle sensible qui aurait pu être transmise en cours de réunion).
3. Modifiez les justificatifs d'accès aux réunions ainsi que les mots de passe des réunions récurrentes ou planifiées.
4. Signalez les activités malveillantes au Centre pour la cybersécurité : contact@cyber.gc.ca.

CONSEILS À L'INTENTION DES EMPLOYÉS

Les formations en cybersécurité constituent des moyens efficaces de protéger votre organisme contre les cybermenaces et d'instaurer une culture organisationnelle axée sur sécurité. Ainsi, il convient de rappeler aux employés les pratiques exemplaires suivantes avant qu'ils n'utilisent les applications de vidéoconférence :

- N'utilisez que les applications de vidéoconférence approuvées à des fins professionnelles.
- N'échangez jamais d'information sensible par l'intermédiaire d'un système de vidéoconférence.
- Gardez confidentiels les justificatifs d'accès et les mots de passe des réunions.
- Utilisez des mots de passe forts dans le cas des comptes.
- Utilisez l'authentification à plusieurs facteurs lorsque c'est possible.
- Entrez l'adresse Web de la vidéoconférence manuellement dans un navigateur Web, ce qui vous évite de cliquer sur des liens potentiellement malveillants.
- Utilisez un réseau sans fil sécurisé.

Prière de consulter notre alerte AL20–011 *Facteurs à considérer pour l'utilisation de produits et services de vidéoconférence*, qui est disponible dans notre site Web.

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**.