LE COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE PUBLIE DES CONSEILS POUR UNE VIDÉOCONFÉRENCE SÉCURISÉE

Publié le 5 mai, 2020

Catégories: Perspectives, Publications

Il va sans dire que l'utilisation de la vidéoconférence par les entreprises atteint un niveau sans précédent, car nombre de celles-ci se sont converties au travail à distance. Cette technologie, comme toutes les autres, présente des risques uniques en matière de cybersécurité et de confidentialité des données.

Conscient de l'essor de la vidéoconférence, le Commissariat à la protection de la vie privée du Canada (le « **Commissariat** ») a publié des conseils pour assurer le respect des lois sur la protection de la vie privée pendant les vidéoconférences. Vous trouverez ci-dessous un résumé des conseils du Commissariat, ainsi que quelques conseils de l'équipe de McMillan spécialisée dans la protection de la vie privée et des données concernant les meilleures pratiques à mettre en œuvre dans le cadre du télétravail.

Appliquer les mesures de diligence nécessaires

Avant de choisir un service de vidéoconférence, les entreprises doivent examiner les politiques de confidentialité et les conditions d'utilisation du service afin de comprendre les pratiques du service en matière de protection de la vie privée et de traitement des données. En particulier, vous devez examiner et comprendre comment le fournisseur de vidéoconférence peut recueillir, utiliser et communiquer les renseignements personnels des personnes qui ouvrent un compte ou participent à une vidéoconférence. Déterminez si ces politiques et conditions d'utilisation sont conformes à la politique de protection de la vie privée, aux conditions contractuelles et aux autres engagements ou obligations de votre entreprise en matière de protection de la vie privée et de traitement des données. Votre entreprise devra peut-être réviser son programme de conformité en matière de protection de la vie privée, y compris sa politique de protection de la vie privée, afin de permettre l'utilisation de la vidéoconférence.

Les utilisateurs du service de vidéoconférence devraient être encouragés à créer et à périodiquement mettre à jour un mot de passe unique et complexe lors de la création d'un nouveau compte dans un service de vidéoconférence. Le Commissariat recommande aux utilisateurs d'éviter d'utiliser des comptes de médias sociaux pour s'inscrire à de tels comptes.

Suivre l'actualité

Les entreprises devraient suivre l'actualité et les publications sur les vulnérabilités de leur service de vidéoconférence en matière de sécurité et de protection de la vie privée.

Nous recommandons aux entreprises d'établir une alerte Google ou d'autres moyens de suivre les mises à jour provenant de sources fiables concernant les vulnérabilités ou les failles signalées dans leur logiciel de vidéoconférence. De cette manière, une entreprise pourra agir rapidement pour installer les correctifs ou les mises à jour nécessaires, ou prendre d'autres mesures pour réduire au minimum les risques de sécurité. Nous suggérons également aux entreprises de mettre à jour leur politique ou leur programme de gestion des correctifs afin d'inclure des tests réguliers, des mises à jour et des correctifs pour tous les services de vidéoconférence.

Les utilisateurs de vidéoconférence devraient également être encouragés à vérifier périodiquement les autorisations de leurs équipements et à s'assurer qu'elles sont à jour.

Limiter le nombre de participants

Les utilisateurs de vidéoconférence doivent s'assurer que les réunions sont privées et limitées aux participants invités.

Abstenez-vous d'annoncer les réunions sur des plateformes de médias sociaux ou des sites Web afin d'éviter que des participants non invités ne se joignent à la réunion et puissent éventuellement entendre des discussions privées. Si possible, assurez-vous que les appels en vidéoconférence sont sécurisés par un mot de passe, particulièrement si les discussions font état de renseignements personnels sensibles. Les hôtes de réunion devraient également désactiver les fonctions permettant la connexion à la réunion avant l'hôte et les transferts de fichiers afin de limiter les risques de sécurité.

Nous recommandons d'effectuer un « appel nominal » au début de la vidéoconférence, en particulier si des utilisateurs qui composent le numéro ne sont pas visibles à l'écran. Cela peut aider à vérifier que toutes les personnes participant à l'appel sont censées être présentes.

Prévenir l'écoute et le partage indus

Le lieu de la vidéoconférence est également important. Les participants doivent s'assurer qu'il n'y a rien en arrière-plan de l'appel qui révèle des informations privées, comme un tableau blanc ou un calendrier affichant des notes confidentielles. S'ils utilisent un navigateur Web, les utilisateurs doivent ouvrir une nouvelle fenêtre pour l'appel et fermer toutes les autres applications, y compris le courriel, afin de s'assurer que des informations confidentielles ne sont pas divulguées par inadvertance si un partage d'écran se produit pendant l'appel.

La vidéoconférence devrait se dérouler dans une zone privée, idéalement une pièce séparée de la maison. Toutefois, pour certains employés, il peut être impossible de prendre un appel dans une pièce privée ou complètement hors de portée des autres membres de leur foyer. Nous recommandons donc à l'hôte de demander à tous les utilisateurs, dès le début de la vidéoconférence, s'ils peuvent être à portée de voix des autres membres de leur foyer pendant l'appel. Ces utilisateurs devraient écouter l'appel au moyen d'un casque d'écoute et devraient être encouragés à envoyer toute contribution contenant des informations confidentielles par courriel de suivi, au moyen d'une fonction de clavardage privé ou lors d'un appel séparé lorsqu'ils se trouvent dans un espace privé.

Les hôtes de réunion doivent désactiver la possibilité pour les participants d'enregistrer un appel. Demandez aux participants de désactiver les assistants personnels à domicile (tels qu'Alexa ou Siri) ou les haut-parleurs intelligents pendant un appel vidéo, car ces technologies peuvent être déclenchées ou pourraient enregistrer l'appel par inadvertance.

Leçons pour votre entreprise

Au vu de la vulnérabilité des services de vidéoconférence aux menaces de sécurité, il est important que les entreprises adoptent les suggestions et les meilleures pratiques développées par le Commissariat.

Toutefois, les conseils qui précèdent ne devraient constituer qu'une partie d'un effort plus large visant à remédier aux vulnérabilités en matière de protection de la vie privée et de cybersécurité causées par le travail à distance.

Les périodes de crise entraînent un risque croissant de cyberattaques et de menaces. Les auteurs de menaces exploitent les vulnérabilités de sécurité, le manque d'attention des employés et la méconnaissance des nouvelles technologies pour tenter d'accéder illégalement à des renseignements commerciaux et personnels sensibles. Les entreprises doivent mettre l'accent sur une culture de la cybersécurité et sur le respect des lois sur la protection de la vie privée et des données afin de réduire au minimum ces risques. Lorsqu'elles forment convenablement leurs employés sur les cyberrisques et qu'elles font des rappels fréquents à ce sujet, y compris sur l'utilisation correcte des technologies de vidéoconférence, les entreprises prennent des mesures importantes pour éviter les atteintes à la protection des données.

Alors que nous attendons tous avec impatience le jour où nous pourrons à nouveau avoir des contacts directs avec nos collègues et nos clients, nombreux sont ceux qui suggèrent que la hausse du travail à distance pourrait bien être durable. Nous conseillons aux entreprises d'agir dès maintenant pour élaborer et mettre en œuvre des politiques et des pratiques qui garantissent la sécurité des renseignements confidentiels et personnels en ces temps incertains.

par Kristen Pennington et Chiedza Museredza

Mise en garde

Le contenu du présent document ne fournit qu'un aperçu du sujet et ne saurait en aucun cas être interprété comme des conseils juridiques. Le lecteur ne doit pas se fonder uniquement sur ce document pour prendre une décision, mais devrait plutôt consulter ses propres conseillers juridiques.