Assurance responsabilité professionnelle Barreau

Février 2021 | Volume 22 | Nº 1

L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique.
Albert Einstein

Service de Prévention

Guylaine LeBrun, avocate
Coordonnateur aux activités de prévention

Judith Guérin, avocate
aux activités de prévention

Les cyberrisques et le télétravail

Depuis le début de la pandémie, on a assisté à une augmentation exponentielle de l'utilisation des technologies de l'information par les cabinets d'avocats, entreprises et autres afin de permettre la continuité des activités. Toutefois, certains risques sont associés à ces technologies lorsque celles-ci ne sont pas nécessairement maîtrisées par l'utilisateur.

Débutons avec les logiciels de vidéoconférence. Que vous utilisiez *Google Hangouts*, *Microsoft Teams*, *Cisco Webex*, *GoTo Meeting* ou *Zoom*, si on ne sait pas comment configurer ni se servir de ces outils en toute sécurité, on risque de contrevenir à nos obligations déontologiques, dont le secret professionnel.

Par ailleurs, les médias ont rapporté des failles liées à l'infiltration de tierces parties non invitées (nommées Zoom-bombing), ou de détournement de réunions de vidéoconférence ayant comme objectif de perturber les activités ou de compromettre les systèmes informatiques.

Selon le Centre canadien pour la cybersécurité,[1] ce type d'infiltration peut se produire, notamment lorsque les réunions sont accessibles sans mot de passe ou lorsqu'elles ne disposent pas de « salle d'attente » grâce à laquelle les participants seraient identifiés avant d'être admis à la vidéoconférence.

D'autres situations inattendues peuvent également se produire si le logiciel utilisé pour les réunions en vidéoconférence n'est pas configuré comme il se doit. À titre d'exemple, des utilisateurs anonymes pourraient, sans y être invités, participer à ces réunions, si les paramètres de configuration ne sont pas correctement appliqués.

D'autant plus, *qu'au-delà du risque évident sur le plan de la confidentialité, une telle infiltration inattendue peut entraîner des*

[1] https://www.cyber.gc.ca/fr/.

atteintes à la réputation, la perte de crédibilité, la perturbation d'activités et par le fait même, la nécessité de rétablir des communications sécurisées selon le Centre canadien pour la cybersécurité. Par ailleurs, on retrouve sur leur site Internet une liste non exhaustive de conseils d'utilisation formulés par les divers fabricants de logiciels de vidéoconférence couramment utilisés afin de permettre en toute sécurité le télétravail associé à ces réunions virtuelles.[2]

Toutefois, attention, c'est un monde en constante évolution. Il est donc recommandé de vérifier les plus récentes mises à jour de ces logiciels avant leur utilisation puisque celles-ci corrigent certaines vulnérabilités décelées. Ainsi, du jour au lendemain, de nouveaux risques pourraient venir tout chambouler. Si vous n'êtes pas bien outillé, vous risquez de compromettre vos activités en toute sécurité.

Poursuivons avec le télétravail. Avec cette pandémie, il va sans dire que le télétravail pose quelques difficultés. En travaillant à distance, nous devons accéder aux applications et aux informations internes dont on se servirait normalement si nous étions au bureau. Certaines situations sont susceptibles de se produire lors de l'utilisation de ces applications et de ces informations, notamment :

- Données internes détruites par piratage ou par un virus;
- Documents confidentiels divulgués à des tiers;
- Virus transmis au client au moment où vous lui envoyez une opinion juridique, paralysant l'ensemble de son système;
- Virus transmis à tous ceux apparaissant à votre carnet d'adresses;
- Document transmis par courriel au mauvais destinataire;
- Usurpation d'identité ou usurpation d'adresse IP.

Par conséquent, autant de situations susceptibles de se produire et de causer des dommages. Cela dit, rappelons que la police du *Fonds d'assurance responsabilité professionnelle du Barreau du Québec* couvre uniquement la responsabilité professionnelle. Ainsi, pour que la garantie puisse s'appliquer, les dommages doivent avoir été causés par le défaut de rendre ou une erreur ou omission en rendant des services professionnels.

Le Fonds d'assurance ne couvre pas les cyberrisques, ces risques faisant l'objet d'une garantie d'assurance de biens et de responsabilité souscrite auprès d'assureurs commerciaux. Il en est de même quant aux coûts de reconstruction d'une banque de données, lesquels devraient faire l'objet d'une police d'assurance de biens.

---

[2] https://cyber.gc.ca/fr/avis/facteurs-considerer-pour-lutilisation-de-produits-et-services-de-videoconference.

Il importe donc de réaliser l'importance des cyberrisques et de vous adresser à vos courtiers d'assurance et assureurs commerciaux afin de souscrire à une police d'assurance qui couvre ces risques. En souscrivant à une telle police d'assurance, vous pourrez aussi bénéficier de conseils d'experts en sécurité de l'information si un cyberrisque devait se matérialiser.

Ainsi, le télétravail comporte sa part de risques. Il est donc primordial de s'assurer que les niveaux de confidentialité et de sécurité attendus soient maintenus lors de la configuration et de l'utilisation de ces logiciels afin d'empêcher toute personne malveillante d'accéder à nos systèmes et de compromettre nos activités. Par conséquent, nous devons mettre en place des mesures de sécurité additionnelles afin d'interdire à tout auteur malveillant de s'introduire et d'exploiter d'éventuelles vulnérabilités de nos systèmes.

Il est donc important d'accéder aux applications et aux informations par le biais d'un réseau privé virtuel (VPN) pour se connecter aux serveurs du cabinet ou de l'entreprise. Par le biais de ce réseau, la connexion est sécurisée puisqu'elle impose un mode d'authentification qui protège les données. Les informations sont donc acheminées de façon sécuritaire tout en étant chiffrées.

Finalement, la vigilance est également de mise quant à la protection des propriétés et métadonnées d'un document. Les avocats ne devraient pas transmettre de documents dont les propriétés et métadonnées sont visibles.

Cela dit, que vous soyez en télétravail ou non, voici donc quelques suggestions :

Mesures d'atténuation des risques
✓ Assurez vos cyberrisques auprès d'un assureur.
✓ Adoptez une *Politique de sécurité de l'information.*
✓ Limitez les privilèges d'accès à vos documents.
✓ Protégez les documents sensibles avec un mot de passe, pour la lecture et la modification.
✓ Utilisez un mot de passe robuste – alphanumérique avec majuscules, nombres et substitution de caractères (exemples : ! = 1, $ = s, @ = a, etc.) ou idéalement une phrase de passe, changez ce mot ou cette phrase de passe aux 3 mois et gardez le tout dans un répertoire chiffré (ou une voute à mots de passe).
✓ Mettez en place les authentifications multifacteurs.

- ✓ Activez votre écran de veille au moins à 10 minutes avec mot de passe.
- ✓ Utilisez un logiciel « Antivirus » ainsi qu'un pare-feu (Firewall) et effectuez les mises à jour régulièrement.
- ✓ Faites des copies de sauvegarde (backup) de vos fichiers et de toutes informations jugées essentielles.
- ✓ Conservez les copies de sauvegarde sous clé, dans un lieu sûr, dans une autre pièce ou autre lieu.
- ✓ N'ouvrez que les pièces jointes (*attachment*) de courriels dont vous connaissez la provenance.
- ✓ Ne cliquez que sur les liens dont vous connaissez également la provenance. Soyez attentif aux courriels et à leur contenu. Contiennent-ils une adresse étrange ou inexacte ou d'autres coquilles de ce genre dans l'orthographe? La moindre distraction peut entraîner un clic sur un lien fatal et c'est déjà trop tard, votre système est infecté.
- ✓ Ne répondez jamais à des courriels indésirables (« *junk mail* » ou « *spam* »).
- ✓ La sécurité informatique est l'affaire de tous à la maison.
- ✓ Déconnectez-vous du serveur à distance si vous vous absentez (par exemple, pour prendre une marche le midi).
- ✓ Choisissez un logiciel de vidéoconférence qui comporte les fonctions nécessaires de sécurité, notamment la possibilité d'imposer l'usage d'un mot de passe fort ou une méthode d'authentification à deux facteurs, ainsi qu'un bon niveau de chiffrement, le tout, permettant de contrôler les accès à la vidéoconférence.
- ✓ En fonction du logiciel utilisé, établissez des règles quant aux types de discussion pouvant être tenus.
- ✓ Organisez régulièrement des réunions virtuelles bien entendu (pandémie oblige), sur des sujets de cybersécurité, comme l'hameçonnage, la gestion de mots de passe et les différents types de cyberattaques afin de sensibiliser votre personnel et les membres de votre équipe.
- ✓ Utilisez les outils qui conviennent le mieux à la tâche visée. Par exemple, expédiez des documents confidentiels par messagerie ou par l'entremise d'une plateforme d'échanges sécurisée.

- ✓ Assurez-vous que les organisateurs de vidéoconférence connaissent les fonctions de sécurité disponibles dans le logiciel utilisé et qu'ils les appliquent correctement. À titre d'exemple, protégez la confidentialité des réunions en exigeant un mot de passe. Si cette mesure ne peut pas être appliquée, contrôlez l'accès des invités au moyen d'une salle d'attente, tout comme nos clients ou visiteurs qui se présentent à nos bureaux.
- ✓ Choisissez de quelle façon les données seront traitées. Certains logiciels peuvent retransmettre les données à l'extérieur du Canada ou conserver ces mêmes données sur des serveurs administrés par des tiers.
- ✓ N'inscrivez aucun lien d'identification de vidéoconférence dans des forums publics ou non gérés.
- ✓ Installez toujours la plus récente mise à jour pour chacun de vos logiciels.

Des mesures internes de sécurité sont trop souvent et facilement négligées. Il n'est donc jamais trop tard pour vérifier la sécurité de vos réseaux informatiques et de tout logiciel de vidéoconférence utilisé. *Faire confiance, c'est négliger sa vigilance*. (Szczepan Yamenski).

Source :

Centre canadien pour la cybersécurité (Gouvernement du Canada) à https://www.cyber.gc.ca/.