Hébergement ASO sur nos serveurs

La sécurité et l'accessibilité des données au cœur de nos préoccupations

Quelle est votre protection contre une cyber-attaque?

Nous faisons affaires avec Microsoft Azure. Microsoft Azure a déjà de nombreuses dispositions anti-cyber-attaque étant donné son infrastructure infonuagique et ses ressources.

Nous utilisons notamment leur pare-feu et nous restreignons l'accès qu'à nos adresses IP et sur autorisation seulement (« on demand only »).

L'identification à deux facteurs est en force pour se connecter à notre infrastructure Azure.

Respectant la loi 25, tous nos accès sont saisis dans un journal de bord et contrevérifiés avec les logs machines et de Microsoft.

Quelle mise à jour faites-vous au niveau de vos serveurs?

Nous procédons aux mises à jour mensuellement de Microsoft SQL Server et Windows Server et maintenant une version supportée de PHP.

Qui peut accéder au logiciel ou aux données?

Seule notre équipe technique a accès aux serveurs via des adresses IP autorisées et sur autorisation seulement. Un registre des entrées est tenu en tout temps.

L'accès aux données se fait par adresse IP reconnue seulement avec code utilisateur et mot de passe et nous recommandons fortement l'authentification à deux facteurs (envoi d'un code sur un cellulaire, par exemple). Par défaut, ASO est configuré pour fonctionner avec Microsoft Authenticator.

Nous tenons des registres d'entrées chaque fois qu'un de nos employés se connecte à une plateforme ASO en production (ex. lors d'une demande de soutien technique)

Est-t-il est possible d'accéder à ASO à l'extérieur du lieu de travail?

ASO est hébergé sur un serveur Microsoft Azure accessible via un navigateur web grâce à une url (adresse web) avec une protection par adresse IP. Il est donc possible d'accéder à ASO à l'extérieur du lieu de travail en autorisant d'autres adresses IP (ex. domicile). La sécurité peut être renforcée par l'authentification à deux facteurs (recevoir un code d'accès sur un cellulaire à saisir lors de l'accès à ASO).

Quelles sauvegardes sont faites et où sont conservées les données?

Nous utilisons la redondance de Microsoft – au Canada seulement et les backups sont pris selon la recommandation de la Chambre des Communes du Canada (sur 14 jours quotidiennement + 1 backup par mois sur 12 mois). Les backups sont eux aussi conservés au Canada.

Le Centre de données principal est au Québec, à Québec, le centre de données de redondance et backup est en Alberta toujours au Canada

Hébergement ASO sur nos serveurs

Que se passe-t-il en cas de panne du serveur principal

En cas de panne du serveur principal empêchant l'utilisation de la plateforme ASO du client, l'url est redirigée vers le serveur de redondance (de sauvegarde). Le délai de redirection est de quelques minutes seulement.

Que se passe-t-il en cas de panne de courant électrique?

Comme ASO est hébergé sur un serveur accessible par internet, même en cas de panne de courant électrique, vous pourrez éventuellement y accéder via un local non affecté par la panne de courant (ex, votre domicile). Cela vous prendra un accès WIFI ou LTE (point d'accès cellulaire) et le système peut être accessible en autorisant simplement l'adresse IP de l'endroit où vous vous trouvez.

Que se passe-t-il en panne d'internet?

Vous pouvez activer une clé LTE ou un routeur LTE qui vous permettra d'utiliser le réseau cellulaire. Ainsi, en cas de panne internet via un wifi, vous pourrez utiliser ASO via le réseau de données cellulaires LTE.