Office of the Auditor General of Ontario
Bureau de la vérificatrice générale de l'Ontario

Volume 1, chapitre 3.13 – Systèmes technologiques (TI) et cybersécurité à la Société des loteries et des jeux de l'Ontario

Audit de l'optimisation des ressources 2019

Pourquoi avons-nous effectué cet audit?

- La Société des loteries et des jeux de l'Ontario (OLG) a versé environ 45 % du total des revenus non fiscaux de 5,47 milliards de dollars générés en 2018-2019 par les entreprises publiques provinciales, qui comprennent également la Régie des alcools de l'Ontario, Ontario Power Generation Incorporated, Hydro One Limited et la Société ontarienne de vente du cannabis.
- Nous n'avons pas effectué d'évaluation des systèmes de TI à l'OLG, pas plus qu'un examen du rendement des fournisseurs et de la cybersécurité.

Pourquoi cet audit est-il important?

- La cybersécurité est une mesure névralgique pour protéger OLG contre les cyberattaques, les atteintes à la vie privée, les atteintes à la réputation et la destruction de l'information et de l'infrastructure essentielles.
- L'interruption des activités d'OLG peut non seulement avoir une incidence négative sur l'expérience des clients de la Société, mais également réduire les revenus de la province.

Nos constatations

- OLG n'a pas toujours tenu à jour ses tests de vulnérabilité de ses systèmes de TI. La Société effectue régulièrement des évaluations de la vulnérabilité, mais elle n'effectue pas de tests périodiques de sécurité comme des tests de pénétration pour ses secteurs d'activité de loterie et de jeux en ligne afin de mieux cerner ses vulnérabilités sur le plan de la cybersécurité. En novembre 2018, un pirate informatique a attaqué le système de jeu en ligne d'OLG, ce qui l'a rendu inaccessible pendant 16 heures et a nui à l'expérience client.
- Sept employés d'OLG ont accès à des renseignements confidentiels non chiffrés sur les clients. Les renseignements personnels des clients d'OLG sont chiffrés pour empêcher leur accès à l'extérieur. Toutefois, ces sept employés d'OLG ont accès aux renseignements sous une forme non chiffrée, ce qui accroît le risque que les renseignements personnels des clients soient consultés à des fins inappropriées. Nous avons également constaté que deux casinos que nous avons visités ne respectent pas les normes de sécurité de l'information d'OLG et ne chiffrent pas les données sur les clients dans leurs systèmes de TI.
- Nous avons constaté qu'OLG ne suit pas les pratiques exemplaires de l'industrie, qui consistent à examiner le code source (la liste des instructions lisibles rédigées par un programmeur) pour repérer les lacunes en matière de cybersécurité dans les systèmes de TI critiques pour ses activités de loterie, de jeu en ligne et de casino.
- Bien que des stratégies de reprise après sinistre aient été élaborées et mises à l'essai pour les systèmes de TI de chaque secteur d'activité, nous avons constaté qu'OLG n'avait pas de stratégie globale intégrant tous les systèmes de TI de façon cohérente, même après un événement important qui aurait dû l'inciter à en préparer une.
- Les indicateurs de rendement pour les services essentiels de TI ne sont pas toujours intégrés à l'entente sur les niveaux de service conclue avec les fournisseurs de TI. Trois des 10 ententes sur les niveaux de service que nous avons examinées n'incluaient pas d'indicateurs clés du rendement en TI. Selon l'entente sur les niveaux de service, un ou plusieurs indicateurs de rendement pour les services essentiels, comme l'accessibilité du système, les pannes de service, la résolution des incidents et les délais d'intervention, n'ont pas été inclus. Cela influe, à divers degrés, sur la mesure de l'expérience client et, éventuellement, sur les revenus et les activités commerciales.
- Certains fournisseurs de TI affichent un rendement inférieur et ne sont pas tenus responsables de l'atteinte des objectifs de rendement. OLG n'examine pas systématiquement le rendement de tous les fournisseurs de TI par rapport à leur entente sur les niveaux de service et ne prend pas de mesures correctives au besoin, par exemple en imposant des amendes conformément à leur entente sur les niveaux de service. Nous avons trouvé des cas où OLG n'avait pas examiné le rendement des fournisseurs de TI.
- OLG a lancé d'importants projets de TI dans ses divers secteurs d'activité. OLG a mis en oeuvre 33 projets de TI dans les limites de son budget, mais les 11 autres dépassaient son budget; cela représente près de la moitié du total des dépenses liées aux projets de TI au cours des cinq dernières années (échantillon de 91 millions de dollars sur des dépenses totales de 232 millions); la Société affichait des retards et des dépassements de coûts de plus de 10 millions de dollars.

..../2

Nos conclusions

- Il est possible de renforcer les pratiques de cybersécurité dans les systèmes de TI. OLG n'effectue pas régulièrement d'évaluations de la sécurité, notamment au moyen de tests de pénétration pour ses secteurs d'activité de loterie et de jeux en ligne afin de mieux cerner les vulnérabilités potentielles.
- Il est possible de renforcer la protection des renseignements sur les clients dans certains systèmes de TI de jeu de l'OLG et de deux casinos.
- OLG doit améliorer sa supervision des fournisseurs de services de TI. Cette mesure est particulièrement importante en raison de la grande dépendance d'OLG à ces fournisseurs. Les contrats de TI d'OLG n'énoncent pas toujours les exigences de rendement nécessaires pour assurer l'exécution efficace des activités.

Le rapport est accessible à l'adresse www.auditor.on.ca