Gestion des systèmes de contrôle industriels

Mise en contexte

La Direction de l'eau potable (DEP) du Service de l'eau (SE) de la Ville de Montréal (la Ville) gère notamment 6 usines de production d'eau potable situées sur le territoire de l'île de Montréal. Elles totalisent une capacité de production de près de 3 millions de mètres cubes d'eau potable par jour, et ce, afin de desservir ses quelques 2 millions de citoyens.

Chaque usine d'eau potable contrôle de manière centralisée leurs équipements par un système de contrôle et d'acquisition de données « *Supervisory Control and Data Acquisition* » (SCADA). De plus, divers autres systèmes informatiques sont utilisés pour la planification, la gestion, le suivi et le contrôle de ces équipements.

Plus que jamais, les villes sont confrontées à des menaces émergentes sous la forme de cyberattaques qui ont pour objectifs de prendre le contrôle, d'endommager ou de détruire des Systèmes de contrôle industriels (SCI), ce qui pourrait perturber ou rendre indisponible l'approvisionnement de l'eau potable et mener à des demandes de rançon de plusieurs millions de dollars.

Il est important de s'assurer que des mesures de sécurité ainsi que des contrôles industriels et technologiques sont en place à la Ville afin de réduire les risques associés à ces menaces.

Objectif de l'audit

Déterminer si les mécanismes mis en place à la Ville permettent une saine gestion ainsi qu'une haute disponibilité des Systèmes de contrôle industriels utilisés par la DEP.

Résultats

De façon globale, nous concluons que la Ville a mis en place des mécanismes permettant une saine gestion et une haute disponibilité des SCI et des technologies de l'information (TI) pour la production d'eau potable.

Cependant, plusieurs éléments nécessitent des améliorations notamment au niveau des encadrements, de la suffisance des ressources TI spécialisées dans le domaine industriel ainsi que de la gestion des actifs informationnels.

Toutefois, compte tenu de la présence de plusieurs contrôles compensatoires, ces derniers éléments n'ont pas d'impacts significatifs sur la disponibilité des SCI et TI de la DEP.

Principaux constats

Encadrement et gouvernance

- Les contrôles industriels de la DEP sont adéquatement documentés, mais il n'y a pas de révision systématique. De plus, il n'y a pas d'encadrements formels TI adaptés à la réalité de l'environnement de la DEP. Il existe un document de partage à haut niveau des rôles et des responsabilités, mais il ne présente pas les rôles et les responsabilités détaillés des parties prenantes dans la gestion des SCI de la DEP.

Suffisance des ressources

- Les ressources en automatisation de la DEP sont suffisantes afin de répondre aux besoins. Toutefois, il y a un manque de ressources TI expérimentées dans le domaine industriel tant au niveau de la DEP que du Service des technologies de l'information.

Gestion des accès logiques

- Il n'existe pas d'encadrements formels de gestion des accès logiques des SCI de la DEP.

Sécurité des réseaux

- Une architecture technologique a été schématisée avec une segmentation adéquate des réseaux. Les équipements de sécurité réseau sont adéquatement configurés. Néanmoins, il n'y a pas d'encadrements formels de gestion des mises à jour des SCI.

Surveillance des systèmes

- Un outil technologique est utilisé afin de surveiller la disponibilité de systèmes et envoyer des alertes aux parties prenantes. Toutefois, cet outil ne couvre pas l'ensemble de ces systèmes. Cette surveillance ne fait pas l'objet d'encadrements formels.

Gestion des changements

- Les changements importants sont généralement documentés dans un outil technologique. Cependant, il n'y a pas d'encadrements formels de gestion des changements et les demandes de changements ne sont pas systématiquement documentées.

En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires qui sont présentées dans les pages suivantes. Ces unités d'affaires ont eu l'opportunité de donner leur accord relativement aux recommandations.