Gestion des systèmes de contrôle industriels

Mise en contexte

La Société de transport de Montréal (STM) fournit à la population de l'île de Montréal des services de transport collectif, dont le service de métro, d'autobus et de transport adapté.

En ce qui concerne le réseau du métro, il comprend 4 lignes desservant 68 stations sur 71 kilomètres. Ceci représente une offre de service de 85,3 millions de kilomètres parcourus annuellement. Le métro est contrôlé de manière centralisée par un Système de contrôle et d'acquisition de données « *Supervisory Control and Data Acquisition* » (SCADA) qui surveille et gère les opérations du métro. Cette gestion nécessite l'utilisation de systèmes de contrôle industriels (SCI) composés de technologies opérationnelles (TO) et de technologies de l'information (TI).

Les SCI, tout comme les systèmes informatiques traditionnels, peuvent être confrontés à des menaces émergentes sous la forme de cyberattaques provoquant des dommages, du vol d'information et de la destruction ou l'altération du bon fonctionnement des SCI du métro.

Le présent rapport traite de nos constatations qui sont de nature publique. Un rapport détaillé distinct a été publié uniquement à l'interne en raison des renseignements hautement sensibles et confidentiels qu'il contient.

Objectif de l'audit

Déterminer si les mécanismes mis en place à la STM permettent une saine gestion ainsi qu'une haute disponibilité des systèmes de contrôle industriels utilisés par le métro.

Résultats

Nous concluons que la gestion des SCI par la Société de transport de Montréal (STM) nécessite des améliorations afin d'assurer une gestion plus efficace et de réduire les risques de perte de disponibilité du métro.

En effet, la gestion inadéquate des accès logiques aux SCI augmente le risque d'accès non autorisés, ce qui pourrait altérer le fonctionnement du métro. De plus, l'absence de plan de relève informatique formel engendre un risque de perte de disponibilité des SCI.

Plusieurs autres éléments doivent être améliorés notamment sur le plan de :

- la formalisation des rôles et responsabilités;
- l'absence de programme de sensibilisation spécifique aux SCI du métro;
- la surveillance des systèmes;
- l'exhaustivité du processus de gestion des changements.

Toutefois, la STM dispose des mécanismes de contrôle adéquats suivants :

- Les ressources humaines de la Division Livraison des services technologiques métro sont suffisantes;
- L'architecture TI/TO est documentée avec une segmentation adéquate des réseaux;
- Les pare-feu sont mis à jour régulièrement.

Principaux constats

Rôles et responsabilités

→ Il n'existe pas de document formel détaillant le partage des rôles et responsabilités afférent aux Systèmes de contrôle industriels du métro.

Suffisance et adéquation des ressources humaines

→ Les ressources humaines en place de la Division Livraison des services technologiques métro sont suffisantes pour répondre à ses besoins.

→ Il n'existe pas de programme de sensibilisation spécifique aux SCI du métro pour les ressources de la Division Livraison des services technologiques métro.

Gestion des accès logiques

→ Les encadrements de gestion des accès logiques ne sont pas adaptés aux SCI du métro ni appliqués systématiquement.

Sécurité des réseaux liés aux environnements industriels

→ L'architecture technologique est documentée et comporte une segmentation adéquate des réseaux.

→ Les pare-feu sont mis à jour régulièrement.

→ Il n'existe pas de procédure formelle d'évaluation et d'installation des mises à jour sur les serveurs SCI.

Surveillance des systèmes

→ Un outil de surveillance et d'alerte d'événements de sécurité est en place. Toutefois, il n'existe pas d'encadrement de surveillance pour les SCI du métro.

Gestion des changements

→ Un processus formel de gestion des changements est appliqué. Cependant, celui-ci est incomplet par rapport aux saines pratiques de l'industrie.

Relève informatique des systèmes

→ Il n'existe pas de plan de relève formel des systèmes informatiques.

En marge de ces résultats, nous avons formulé différentes recommandations aux unités d'affaires qui sont présentées aux pages suivantes.