Cybersécurité

Protéger nos infrastructures en eau

PAR **STÉPHANIE PETIT**
Ph. D., coordonnatrice du secteur Eau,
Réseau Environnement et SQAWWA

PAR **ÉRIC WALKER**
Ingénieur automatisation, PMP, CCNA,
Ville de Laval

PAR **FRANÇOIS TURBIDE**
Chef d'équipe, sécurité des SCI,
Sécurité publique Canada

ET PAR **ROBERT NASTAS**
Président, PM SCADA

Les infrastructures en eau des municipalités sont désormais la cible d'attaques réalisées par des cyberterroristes. Ils souhaitent ainsi ébranler la confiance du grand public et rendre vulnérables ces infrastructures essentielles. Face à cette menace grandissante, affectant les systèmes d'approvisionnement en eau et d'assainissement, sommes-nous prêts ?

Une table ronde sur le thème *Sécurité informatique des infrastructures d'eau : menaces et nouveau défi* a eu lieu lors du Symposium sur la gestion de l'eau, organisé le 10 octobre dernier par Réseau Environnement à Saint-Hyacinthe. Voici un résumé des différents éléments qui ont été abordés.

Des cyberattaques de plus en plus envahissantes

Les récentes cyberattaques visant les organisations municipales et les secteurs de l'eau et de l'énergie au Canada, aux États-Unis et en Europe rappellent qu'aucun pays n'est à l'abri de cette menace. Par ailleurs, les petites municipalités sont souvent prises pour cible et constituent un terrain d'entraînement. En 2016, une usine de traitement d'eau potable aux États-Unis a été sous l'emprise de pirates informatiques ayant infiltré le système de contrôle des automates programmables, et ce, pendant 60 jours. De nombreuses fonctions informatiques critiques, technologies opérationnelles et systèmes bureautiques fonctionnaient en effet sur un seul système, et il en a résulté un dérèglement des vannes et des quantités de produits chimiques utilisés pour le traitement. Selon le rapport d'enquête judiciaire de Verizon, de nombreuses autres activités sont passées inaperçues, notamment le vol de plus de 2,5 millions d'enregistrements de données uniques.

En 2018, Wasaga Beach et Midland, en Ontario, ainsi que la MRC de Mékinac et la Ville de Saint-Tite, au Québec, ont été tour à tour victimes d'hameçonnage et de demande de rançons en cryptomonnaie. Plus récemment, une semaine après que l'ouragan *Florence* ait frappé la côte est des États-Unis cet automne, la Onslow Water and Sewer Authority a été piratée, limitant de façon critique le fonctionnement des services d'eau pendant une telle période de crise.

Mise en place d'un programme de cybersécurité à la Ville de Laval

Des accès inappropriés du personnel, des périphériques réseau en fin de vie, une configuration par défaut, des pratiques d'administration à distance non sécurisées, ou encore une mauvaise surveillance sont autant d'attitudes à risque présentement observées dans différentes organisations municipales.

Après avoir évalué différentes méthodologies et divers standards, le Service de la gestion de l'eau de la Ville de Laval a élaboré un programme sur cinq ans pour sécuriser l'infrastructure informatique des unités du Service de la gestion de l'eau. En effet, à la suite de différentes lectures et d'un audit de la vérificatrice générale, il a été conclu que le protocole de communication devait être sécurisé. Mais par où commencer ?

Le ministère de l'Environnement et de la Lutte contre les Changements climatiques recommande différentes mesures

CINQ MYTHES EN CYBERSÉCURITÉ

1. Je ne fréquente pas les sites dangereux et je vérifie les liens, je suis donc sécurisé.
   - FAUX : c'est le navigateur Web qui est vulnérable. Évitez l'accès Internet direct à partir de réseaux protégés.
2. Nos systèmes sont spécialisés (SCADA/ICS) et sont conçus pour notre organisation, nous sommes donc sécurisés.
   - FAUX : les systèmes SCADA/ICS sont bien connus, et les détails sont disponibles sur Internet.
3. Nous avons un pare-feu, alors nous sommes protégés.
   - FAUX : les personnes autorisées, en effectuant leur travail légitime, sont la plus grande vulnérabilité (poste de travail, hameçonnage, média amovible, etc.).
4. Il n'y a pas de risque, nous ne sommes pas reliés à Internet.
   - FAUX : les brèches et les infections ne suivent pas de convention (média amovible).
5. Nous pouvons avoir confiance en nos fournisseurs et en nos intégrateurs externes pour mettre en place des systèmes sécurisés.
   - ATTENTION : les composants matériels et logiciels nécessaires à la protection adéquate des systèmes informatiques coûtent assez cher, et le contractant ne les fournira pas (à moins d'en faire la demande) afin d'avoir des prix concurrentiels.

afin de lutter contre la cybercriminalité dans son *Guide de bonnes pratiques d'exploitation des installations de distribution d'eau potable*, notamment de se référer aux normes et aux documents de l'American Water Works Association (AWWA) et du National Institute of Standards and Technology (NIST). Un outil d'autoévaluation a alors été réalisé, en rassemblant l'information auprès des différents services (système de contrôle, procédés, comptabilité, ressources humaines, etc.), mais aussi auprès de certains vendeurs et fournisseurs. L'utilisateur de l'outil doit passer en revue les informations spécifiques relatives aux systèmes de contrôle des processus de l'entreprise, notamment l'inventaire des périphériques, l'architecture réseau, les fonctionnalités logicielles, les installations physiques et l'architecture des processus de l'usine. Le NIST, dans son cadre de base de la cybersécurité (*Framework for Improving Critical Infrastructure Cybersecurity*), décline en cinq aspects les priorités à étudier pour assurer une sécurité des systèmes, soit l'identification du matériel et des outils sur le réseau, l'élaboration de mesures de protection appropriées pour assurer le service, la mise en œuvre d'activités appropriées pour identifier une défaillance, le développement de mesures pour répondre à un incident, et un plan de résilience pour restaurer des capacités ou des services altérés. La priorité est de segmenter, c'est-à-dire de s'assurer que les réseaux de contrôle soient complètement indépendants du reste des services de la municipalité ; à la Ville de Laval, chacune des usines est indépendante. La gestion des usagers, la mise à jour des systèmes, les sauvegardes, ainsi que la formation des opérateurs et des gestionnaires sont d'autres priorités.

Assurer la sécurité et la résilience des infrastructures

Puisque les catastrophes surviennent habituellement à l'échelle locale, ce sont majoritairement les propriétaires, les exploitants, la municipalité, la province ou le territoire qui sont les premiers à réagir. Au Canada, le gouvernement fédéral a des responsabilités en ce qui a trait à la gestion des urgences. Il est crucial de déployer des efforts et d'établir des partenariats en vue d'accroître la résilience des systèmes d'infrastructures essentielles et de planifier des actions en cas de perturbations imprévues, et ce, pour assurer la prestation de ces services et garder les communautés en sécurité. À cette fin, le gouvernement a accordé à Sécurité publique Canada 1,4 million de dollars en 2018-2019 afin de poursuivre les activités du Programme d'évaluation de la résilience régionale et de la Cellule pour l'analyse virtuelle des risques. Ces programmes soutiennent les évaluations des installations faisant partie de l'infrastructure essentielle, comme les réseaux de technologies de l'information et des communications, et font la promotion de l'échange de renseignements à l'échelle de la communauté des infrastructures essentielles. Le Centre canadien pour la cybersécurité a, quant à lui, le rôle d'informer sur les questions de cybersécurité, ainsi que d'offrir des conseils ciblés, des directives précises et de l'assistance pratique directe, tout en créant des partenariats solides.

À la recherche de conseils ?

Les achats de biens et d'équipements par les municipalités peuvent contenir des aspects technologiques parfois inattendus, tels que la communication par réseau d'affaire ou Internet. Il est fortement encouragé d'inclure, dans tous les contrats et les appels d'offres, une clause concernant l'adhésion aux pratiques exemplaires en matière de cybersécurité, et de lier ces clauses aux pratiques de sécurité informatique et de l'information. Polices d'assurance, réponse aux demandes de rançons, test d'intrusion sont bien d'autres aspects à considérer dans l'établissement d'un programme de sécurisation informatique des infrastructures.

La cybersécurité est un processus continu, tout comme la santé et la sécurité au travail ; il est donc important de constamment s'informer et demander conseil. Symposiums, ateliers techniques et exercices sur table sont d'ailleurs développés par le gouvernement fédéral, et il est aujourd'hui possible de solliciter l'équipe de la sécurité des systèmes de contrôle industriels (SCI) de Sécurité publique Canada. Vous voulez développer une telle communauté de pratique au Québec ? Contactez nos auteurs ! ●

SOURCES À CONSULTER

- ANSI / ISA 62443 Standards to Secure Your Control Systems
- AWWA G430-14 Security Practices for Operation and Management
- Centre canadien pour la cybersécurité (www.cyber.gc.ca)
- Clauses contractuelles visant l'équipement et les services de télécommunications (https://www.cse-cst.gc.ca/fr/system/files/pdf_documents/tscg-ccat01l-fra_1.pdf)
- Infrastructures essentielles, Sécurité publique Canada (www.securitepublique.gc.ca/ci)
- *Framework for Improving Critical Infrastructure Cybersecurity*, NIST
- GRC – *Rançongiciels* (http://www.rcmp-grc.gc.ca/scams-fraudes/ransomware-rancongiciels-fra.htm)
- *10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks*, WaterISAC, Octobre 2016
- « Top 10 Cybersecurity myths », *EMA's Communicator magazine*, N° 1, 2014 (www.awwa.org)