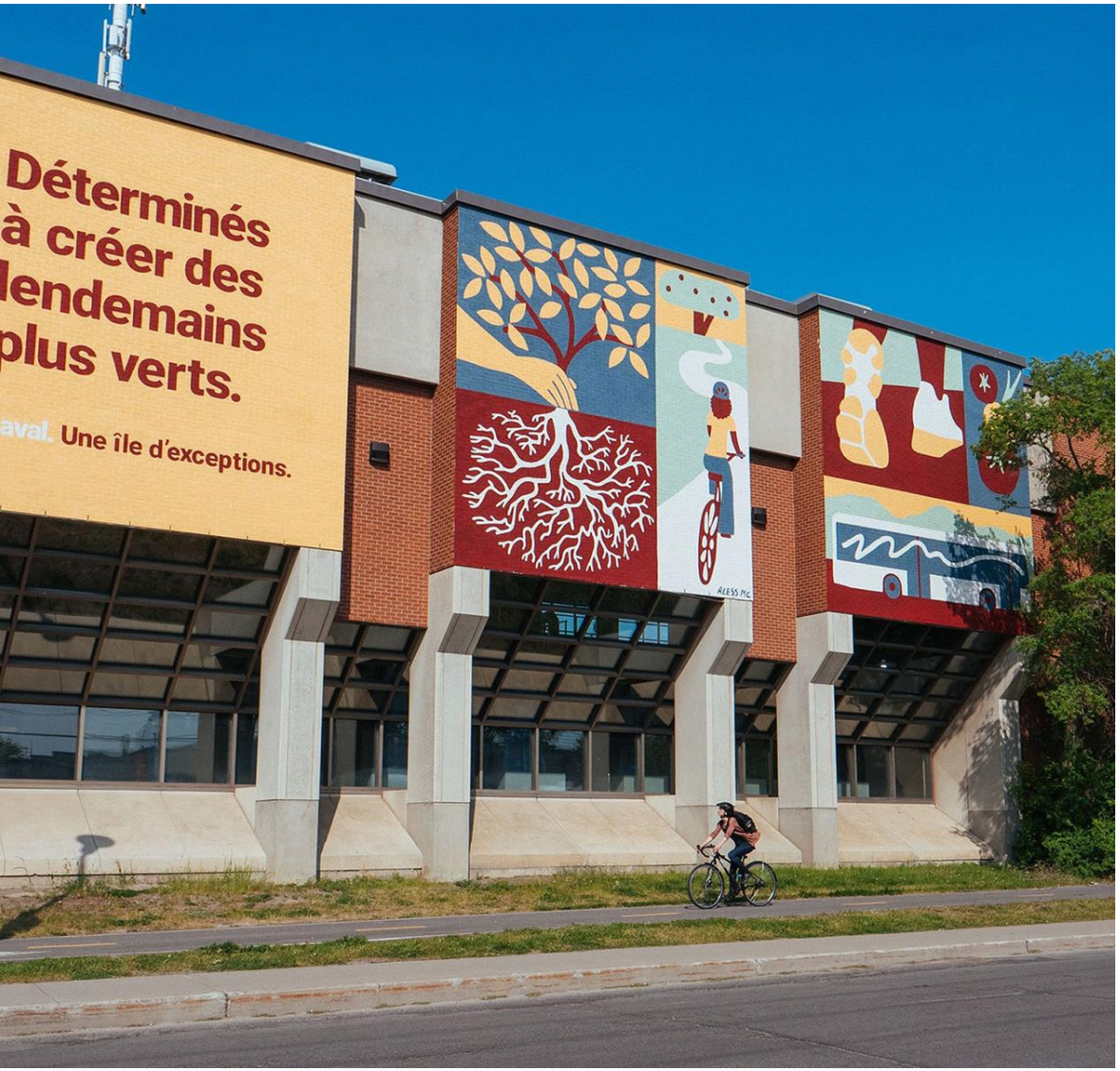

25 janvier 2024

Partage d'expérience suite à une tentative de cyberattaque

Keven Labelle, Conseiller

Bureau de la résilience municipale

Déroulement en deux temps

Faits saillants de l’intervention; de sa détection jusqu’au retour à la normale des systèmes

Comment l’organisation municipale a fait face à cette situation afin de maintenir la prestation de services aux citoyens

Contexte

- Le mercredi, 14 septembre 2022, la Ville de Laval a été victime d’une tentative de cyberattaque;

- Nos activités de surveillance ont cependant permis de détecter cette menace.

Aperçu de la chronologie des évènements

	Détection de la menace	Actions urgentes	Coordination	Intervention	Rétablissement
TEMPS	• Jour 1 - 6h00	• Jour 1 - 11h00	• Jour 1 - 15h00	• 15 au 22 septembre	• 23 au 26 septembre • 31 octobre au 25 novembre
RÉSUMÉ DES ACTIONS	• Alerte avisant d'un trafic anormal de données	• Mesures de mitigation (isolé, etc.)	• Mise en place de cellule de crise SIT • Liaison avec la Direction Générale et le Bureau de la résilience municipale	• Arrivée de l'équipe DART de Microsoft • Activation des mesures de résilience	• Retour progressif des services • Correctifs et améliorations

Détection de la menace

Jour 1 / 14 septembre 2022 / 6h00

- Alerte nous avisant, entre autres, d’un trafic anormal de données, pouvant signifier que la ville de Laval subissait une cyberattaque et que nous pouvions être victime d’exfiltration de données;
- Un compte administrateur avec hauts privilèges avait été également piraté;
- 3 serveurs de courriels semblaient avoir été également compromis.

Actions urgentes

Jour 1 / 14 septembre 2022 / 11h00

- **Désactivation** d'une série de comptes administrateurs à hauts privilèges;
- Changement de **mot de passe**;
- **Déconnexion** de notre réseau des 3 serveurs de courriels;
- Début du **déploiement de l'outil Microsoft Defender** pour point de terminaison sur nos équipements (serveurs et postes de travail)

Coordination

Jour 1 / 14 septembre 2022 / 15h00

Mise en place d'une cellule de crise SIT pour objectif d'éliminer la menace de Cyberattaque;

Actions:

- Désactiver nos liens internet;
- Désactiver le service d'accès à distance (VPN);
- Déconnecter et isoler de notre réseau tous les équipements infectés connus à ce jour.

Coordination (suite)

Liaison avec la Direction Générale et le Bureau de la résilience municipale pour assurer:

- Une coordination organisationnelle de l’événement;
- L’accompagnement des services dans la mise en place de leurs plans de continuité des activités;
- Les communications requises.

Intervention

Jour 2 / 15 septembre 2022 / 14h00

Arrivée de l'Équipe DART de Microsoft avec pour mission:

- Éliminer la menace;
- Assister nos équipes pour les déploiements des outils de surveillance et de collecte de données;
- Analyser les données, poser un diagnostic;
- Fournir des recommandations et préciser les actions requises pour colmater nos failles.

Stratégie d’intervention de l’équipe DART

- Analyse approfondie de notre environnement (Deep scan);
- Surveillance en continu : Déploiement des outils Defender et Sentinel (SIEM);
- Intelligence enrichie : Surveillance de niveau expert (tirer profit de l’expertise mondiale de Microsoft) / Analyse des alertes pour garantir que la menace soit détectée correctement;
- Confinement de l’attaque : Réinitialisation de mots de passe / Désactivation de certains comptes / Mise hors ligne de certains systèmes;

Intervention (suite)

Du 15 au 22 septembre 2022

- Collecte et analyse des données par l’équipe DART
- Recherche des indices de compromissions (IOC)
- Recherche du client 0

Retour progressif des services:

- Assurer le fonctionnement des applications en mode local;
- Rétablissement des serveurs compromis

Rétablissement (Phase 1)

Du 23 au 26 septembre 2022

- Rétablissement des accès à distance;
- Rétablissement de l’accès complet à TEAMS et Outlook en mode local;
- Rétablissement des liens internet.

Retour normal des services: 26 septembre 2022

Rétablissement (Phase 2)

Du 31 octobre au 25 novembre 2022

Équipe **CRT** de Microsoft

- **Assurer** la planification, la mise en scène et **l'expulsion rapide des attaquants** selon :
  - ✓ *l'étendue de leur contrôle connue;*
  - ✓ *les comptes identifiés;*
  - ✓ *les portes d'entrée dérobées;*

- **Fournir un niveau minimal de couches de protection** et de **détection** pour aider à prévenir une potentielle re-compromission et pour **augmenter** la probabilité d'une **détection immédiate** si l'attaquant réussit à réintégrer l'environnement;

Bons coups

LES ACTIONS RAPIDES de l'équipe SIT de la Ville de Laval ont empêché un événement potentiel de rançongiciel qui aurait pu entraîner la mise hors ligne de plusieurs services publics critiques;

- **Mise en place des cellules de crise notamment:**

  - ✓ ***Gouvernance SIT*** *(Direction SIT, coordonnateurs opérations, Microsoft)*

  - ✓ ***Coordination technique*** *(équipe DART, équipes infra SIT, équipe sécurité)*

- Les compétences, la disponibilité et la connaissance de nos ressources internes.

Difficultés et leçons apprises

- **Compréhension du rôle** et mandat de DART par nos équipes internes et notre équipe de sécurité
- **Réaligner nos ressources** sur les objectifs visés
- Outils de **suivi d'avancement** de nos actions
- Mieux **communiquer** à l'ensemble de nos employés
- **Documentation** manquante / Difficulté d'avoir le portrait exact de nos actifs
- **Désuétude** de nos technologies
- **Essoufflement** de nos ressources dû à **l'expertise unique** et **spécifique** de certaines ressources.

Coordination transversale

Un aperçu

Contexte

- Incident majeur d’ampleur « Ville »
- Enjeux directs de continuité des services et de réputation
- Mobilisation de l’ensemble des gestionnaires
- Évaluer la situation requiert du temps
- Limitations au niveau des communications

Impacts transversaux

- À la suite de la réalisation des actions immédiates requises, certains systèmes et/ou fonctions informatiques sont devenus non fonctionnels ou partiellement fonctionnels;

- Les services concernés ont dû mettre en place des plans de continuité afin de livrer les services aux citoyens et employés.

Impacts services essentiels

En aucun cas la sécurité du public n’a été compromise

Impacts services aux citoyens

Services électroniques et systèmes non disponibles ou partiellement disponibles :

- Échanges non fonctionnels (paiements, permis en ligne)
- Consultation du rôle d’évaluation foncière
- Réservation de plateau sportif

Impacts services administratifs

Impossibilité d’accéder à certains systèmes pour les personnes en télétravail;

- Requêtes citoyennes (2e ligne)
- RH – dépôt de candidature, transfert de fichier
- Outils de communications
- Gestion de sommaires décisionnels
- Approvisionnement

Facteurs de succès

- Clarté des rôles
- Établir les priorités
- Experts et vulgarisateurs
- Communications fréquentes
- Proximité de la direction générale
- Préparation des services en amont

Difficultés

- Inconnus et incertitudes
- Soucis de transparence versus le risque du passage à l'acte du pirate
- Certains directeurs peu familiers:

– à la gestion d'incident;

– aux opérations.

- Canaux de communications intra-services

Pistes d’améliorations

- Démarche de planification de continuité
- Structure de gestion des perturbations

Merci

Des questions?