FÉDÉRATION QUÉBÉCOISE DES MUNICIPALITÉS

M. Dominique Chartier, MAP ADO
Directeur des projets spéciaux, responsable du programme de cybersécurité de la Fédération québécoise des municipalités

Serez-vous la prochaine municipalité victime d'une cyberattaque ?

Comme gestionnaires, nous sommes quotidiennement appelés à assurer le bon déroulement de nos projets, à prioriser l'allocation de nos ressources et à anticiper les risques qui pourraient mettre en péril les missions critiques de notre organisation.

Forts de notre expérience et de nos succès dans divers domaines, nous nous fions à eux pour détecter les signes avant-coureurs d'événements qui mériteraient notre attention pour prévenir un dérapage potentiel.

Mais face à un risque que l'on dit imminent et qui, selon notre expérience nous semble mineur, voire inexistant, comment pouvons-nous nous positionner ?

« **Les signes avant-coureurs d'une cyberattaque sont majoritairement inexistants.** »

« **La frappe qui est souhaitée fatale par les cybercriminels est le point culminant d'un long processus silencieux d'infiltration.** »

Tous les experts s'entendent sur le fait qu'en cybersécurité, l'axe d'analyse du risque n'est pas de savoir **si** l'on va être attaqué, mais plutôt **quand.**

Selon le Centre canadien pour la cybersécurité, les cyberattaques vers les organismes publics sont en croissance et le seront encore pour les deux prochaines années[1]. Le temps joue donc contre nous.

Malgré la probabilité élevée et croissante du risque et l'importance de l'impact, pourquoi nos organisations municipales mettent-elles autant de temps à se protéger adéquatement ?

10 contextes de gestion qui contribuent à remettre à plus tard les actions prioritaires en cybersécurité :

Priorisation budgétaire : nos organisations municipales doivent composer avec des budgets limités, on le comprend bien. Et il en va de même pour l'ensemble de leurs services. Cependant, si l'objectif final de la cybersécurité n'est pas perçu comme une priorité et que l'on saisit mal le fait qu'elle sert à protéger horizontalement l'intégrité de tous les actifs informationnels, elle sera malheureusement reléguée en arrière-plan au profit d'autres dépenses immédiates jugées plus urgentes.

Absence de sensibilisation : si nos équipes de gestion n'ont pas eu l'occasion d'être sensibilisées aux dangers et aux conséquences d'une cyberattaque pour leur service, elles seront naturellement portées à sous-estimer leur importance.

Expériences passées : si l'organisation n'a jamais été victime d'une cyberattaque ou si les incidents précédents ont été mineurs, on pourrait se trouver dans un faux sentiment de sécurité, pensant ne pas être une cible potentielle. Il ne faut pas perdre de vue que la majorité des organisations qui ont subi une cyberattaque d'envergure en était à leur premier événement majeur.

Complexité technologique : face à l'évolution rapide des technologies et des menaces, il est possible de se sentir dépassé et de choisir de ne pas s'engager activement dans des stratégies de cybersécurité perçues comme complexes ou inaccessibles.

Pressions opérationnelles : dans certains cas, les besoins logistiques et d'accessibilité peuvent être privilégiés au détriment de la sécurité. Par exemple : faciliter l'accès à distance pour un ou des employés sans mettre en place les protocoles de sécurité jugés contraignants.

Conflits de priorités : on peut faire face à d'autres crises ou priorités immédiates qui détournent notre attention de la cybersécurité.

Méconnaissance des ressources disponibles : nous pouvons ne pas être au fait des ressources ou des outils disponibles pour les municipalités afin d'améliorer la cybersécurité.

Croyance en des solutions magiques : selon plusieurs publicités sur le Web, il serait possible qu'un simple antivirus puisse résoudre tous les risques de cybersécurité, laissant croire à tort, la nécessité d'une approche globale et stratégique pour notre organisation.

Culture d'entreprise : dans certaines organisations, la culture peut être réactive plutôt que proactive. Dans ce cas, des mesures sérieuses ne sont malheureusement prises qu'après qu'un incident s'est produit.

Confiance excessive en des tiers : si une organisation municipale impartit certains de ses services TI, on pourrait croire à tort que la responsabilité de la sécurité repose entièrement sur le fournisseur externe.

[1] https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024.

Alors, que faire pour activer le dossier cybersécurité de son organisation ?

Voici les activités prioritaires, par ordre d'importance, que vous devriez envisager pour réduire les risques en cybersécurité :

Évaluation et identification des risques : il est crucial de repérer et d'évaluer les risques. Cela inclut un inventaire à jour de vos actifs informationnels critiques, les points d'entrée possibles pour les cybercriminels, votre empreinte numérique dans le *dark Web* et l'évaluation des vulnérabilités existantes, dont les pratiques organisationnelles.

Formation et sensibilisation du personnel : les employés sont souvent le maillon le plus faible quand il est question de cybersécurité. Adhérez à un service de formation professionnelle en ligne pour sensibiliser tout le personnel aux meilleures pratiques en matière de cybersécurité et aux signes avant-coureurs des tentatives d'hameçonnage ou d'autres cyberattaques.

Mise en place de protocoles et de politiques de sécurité : créez et instaurez des politiques claires concernant la gestion des mots de passe, l'utilisation d'appareils personnels, l'accès aux systèmes et données, etc.

Mise à jour et maintenance des systèmes : assurez-vous que tous les logiciels, systèmes d'exploitation et infrastructures sont régulièrement mis à jour. Les cybercriminels exploitent souvent les vulnérabilités des systèmes d'exploitation et des logiciels obsolètes.

Plan de réponse aux incidents : mettez en place un plan détaillé pour réagir efficacement en cas de cyberincident. Cela devrait inclure les communications internes, l'approche technique pour isoler rapidement le problème, les étapes de récupération des données et la remise en service des opérations critiques.

Sauvegarde des données : assurez-vous que toutes les données essentielles sont régulièrement sauvegardées et stockées en toute sécurité, de préférence hors ligne ou dans un cloud sécurisé, pour vous prémunir des impacts des attaques par rançongiciel.

Gestion des accès : limitez l'accès aux systèmes et aux données sensibles au personnel nécessaire et qualifié. Utilisez une authentification à deux facteurs et d'autres mesures comme la mise à jour régulière des mots de passe pour renforcer la sécurité des comptes.

Collaboration avec des experts : si la municipalité n'a pas d'expertise interne en cybersécurité (bien distincte de l'expertise en TI), envisagez de collaborer avec une entreprise qualifiée pour bénéficier de compétences élargies sur les aspects de la protection et de la gouvernance en cybersécurité.

Surveillance constante : utilisez des outils et des services de surveillance, de détection et de remédiation 24/7 pour déceler toute activité suspecte dans vos systèmes et assurer une intervention rapide (dans la demi-heure), le cas échéant.

Évaluation régulière : les cybermenaces évoluent constamment. Organisez des évaluations régulières de votre posture de sécurité pour repérer les nouvelles vulnérabilités et ajuster les protocoles en conséquence.

En conclusion

Les enjeux en cybersécurité sont une priorité pour tous les organismes publics, quelle que soit leur envergure. Il est plus que jamais essentiel d'adopter une attitude proactive en matière de cybersécurité, d'inculquer une culture de vigilance au sein de notre organisation et de garantir que les ressources nécessaires sont allouées pour maintenir un niveau de sécurité adéquat.

Pour toute assistance en matière de cybersécurité municipale, n'hésitez pas à contacter le service de cybersécurité de la FQM.

fqm.ca/cybersecurite