Meilleures pratiques en matière de cybersécurité municipale

Soutenir la résilience des municipalités canadiennes

TECHNATION[CA]

À propos de

TECHNATION

TECHNATION est le pont entre l'industrie et le gouvernement dans le domaine de la prospérité technologique au Canada. À titre d'organisme sans but lucratif dirigé par ses membres, TECHNATION rallie le secteur des technologies, les différents paliers de gouvernement et les collectivités du Canada pour favoriser la prospérité technologique d'un océan à l'autre. TECHNATION soutient la prospérité technologique en offrant des occasions de promotion, de perfectionnement professionnel et de réseautage à l'échelle de l'industrie et du gouvernement; en mettant en contact les entreprises canadiennes en croissance et les dirigeants technologiques mondiaux; en mobilisant la chaîne d'approvisionnement mondiale; et en alimentant le bassin de talents dans le secteur des technologies.

TECHNATION est depuis plus de 60 ans le porte-parole national officiel de l'industrie des technologies de l'information et de la communication (TIC), qui représente 210 milliards de dollars. Plus de 43 200 entreprises canadiennes des TIC créent et fournissent des biens et services qui contribuent à créer une société plus productive, plus concurrentielle et plus novatrice. Le secteur des TIC génère plus de 666 500 emplois directs et indirects et investit 7,5 milliards de dollars par an en recherche et développement, soit plus que tout autre acteur du secteur privé.

www.technationcanada.ca

Développement de la main-d'œuvre de demain chez TECHNATION

La prospérité du Canada repose sur une main-d'œuvre numérique qui possède les compétences nécessaires pour s'assurer que nos entreprises et notre pays demeurent concurrentiels dans un marché mondial en constante évolution. TECHNATION développe les talents en numérique, que ce soit dans l'industrie ou en dehors de celle-ci, grâce à un mélange de programmes d'amélioration des compétences et de requalification. En tant qu'outil stratégique de TECHNATION, le développement de la main-d'œuvre de demain a pour objectif de constituer le bassin de main-d'œuvre dont le Canada a besoin pour être en tête de l'économie numérique. Il vise notamment à encourager les jeunes à faire carrière dans les technologies, à conseiller sur les exigences et les résultats d'apprentissage de l'éducation technique, à guider ceux qui œuvrent dans des domaines non techniques ou les groupes sous-représentés vers l'obtention des compétences nécessaires pour se lancer dans une carrière en technologies, à encourager la diversité dans l'industrie, et à contribuer à façonner une politique publique visant à appuyer, à accroître et à améliorer la main-d'œuvre technologique au Canada.

Remerciements

Professionnels de l'industrie de la cybersécurité

TECHNATION souhaite exprimer sa sincère gratitude aux professionnels et aux intervenants de la cybersécurité qui ont contribué directement ou indirectement à l'élaboration du présent document sur les meilleures pratiques par l'intermédiaire d'entretiens, de consultations et de discussions informelles. Bien qu'ils soient trop nombreux pour pouvoir les nommer individuellement, nous sommes sincèrement reconnaissants de l'intérêt et de l'expertise que les membres engagés de la communauté de cybersécurité ont apportés tout au long de ce projet. Leurs points de vue et leurs perspectives ont été essentiels aux résultats. Nous les remercions d'avoir partagé avec nous leur temps, leurs connaissances, leurs recherches et leurs expériences. Nous attendons également avec impatience leurs futures contributions au processus de révision afin que le guide des meilleures pratiques municipales demeure à jour et pertinent. Veuillez consulter l'annexe A pour la liste complète des participants de l'industrie.

Dirigeants, personnel et associations municipaux

TECHNATION tient également à remercier, pour leur contribution et leur mobilisation, les participants à ses événements portant sur les meilleures pratiques en matière de cybersécurité municipale. Leurs commentaires ont été déterminants dans l'élaboration du contenu du présent document. Nous tenons à remercier tout particulièrement la municipalité de Stratford, l'Association des municipalités de l'Ontario (AMO), l'Association canadienne des administrateurs municipaux (ACAM), la Fédération canadienne des municipalités (FCM) et l'Association des systèmes d'information municipale (ASIM) du Canada pour leur soutien à la communication de l'importance de la cybersécurité aux dirigeants municipaux du pays.

Gouvernement du Canada

Ce projet est financé en partie par Sécurité publique Canada dans le cadre de son Programme de coopération en matière de cybersécurité. Les opinions et interprétations contenues dans la présente publication sont celles de l'auteur et ne reflètent pas nécessairement celles du gouvernement du Canada.

Canada

Lignes directrices sur les meilleures pratiques en matière de cybersécurité municipale

Ces dernières années, les administrations municipales ont fait face à des menaces croissantes de cybercriminalité.

Malheureusement, les petites et moyennes municipalités sont les plus susceptibles de faire face à des cybermenaces résultant de la cybercriminalité. Les municipalités peuvent être ciblées dans le but d'obtenir des renseignements sur leurs résidents ou l'accès à des services de paiement et gouvernementaux, ou par le biais de rançongiciels et d'autres perturbations. Ces lignes directrices visent à aider les dirigeants municipaux à comprendre les mesures qu'ils doivent prendre avant tout cyberincident pour se parer à cette éventualité, ainsi que les mesures qu'ils peuvent et devraient prendre après un incident.

Elles ne sont pas de nature technique, et les organisations qui cherchent des conseils sur les mesures techniques appropriées devraient consulter la page *Contrôles de cybersécurité de base pour les petites et moyennes organisations* ou d'autres publications pour déterminer les mesures techniques et les contrôles de cybersécurité appropriés.

Ce qui suit est une ébauche des meilleures pratiques élaborées dans le cadre d'un effort de collaboration lors de deux événements TECHNATION (20 novembre 2020 et 10 mars 2021) et soutenues par des experts en la matière de nos partenaires de l'industrie et gouvernementaux chez RSA, Tenable, Bennett Jones, eSentire, CyberNB, Douglas Communications Group et la Police provinciale de l'Ontario.

Planification préalable aux incidents

Évaluation des menaces et des risques

L'évaluation des menaces et des risques est la principale activité qui vous permettra de vous assurer d'investir judicieusement dans la cybersécurité, en plaçant l'argent et les ressources là où ils peuvent avoir le plus d'effet.

1. **Déterminez ce qui est essentiel pour votre municipalité.** Déterminez les renseignements, les systèmes d'information et les systèmes opérationnels critiques sur lesquels votre municipalité s'appuie. Si l'information ou le système n'est pas critique, cela ne signifie pas qu'il ne doit pas être protégé, mais simplement qu'il ne doit pas être votre priorité.

2. **Identifiez les menaces (accidentelles et délibérées) qui pèsent sur vos renseignements et vos systèmes d'information dans votre contexte municipal.**

   - Participez aux événements de cybersécurité de l'industrie/du secteur.
   - Tirez parti des renseignements des fournisseurs de sécurité liés à votre industrie.
   - Envisagez d'adhérer à Échange canadien de menaces cybernétiques.
   - Consultez régulièrement les sites Web et les alertes de cybersécurité du gouvernement, comme les *Alertes et avis* du Centre canadien pour la cybersécurité ou le *Centre antifraude du Canada*.

3. **Identifiez les risques que les cybermenaces font peser sur vos renseignements, vos systèmes d'information et vos systèmes opérationnels critiques.** Cela vous permettra de classer vos risques par ordre de priorité et vous guidera vers les endroits où vous devez investir les fonds et les ressources dont vous disposez.

4. **Demandez de l'aide.** Si vous ne disposez pas de l'expertise ou des ressources nécessaires, faites appel à des services gérés de cybersécurité ou à d'autres services de tiers pour vous aider.

Planification et gouvernance

1. **Optimisez la sensibilisation et la formation.** Il existe toute une gamme d'activités de formation et de sensibilisation que vous pouvez mener au sein de votre organisation et qui aideront vos dirigeants et vos employés à prévenir les incidents de cybersécurité et à mieux s'y préparer. Il s'agit notamment de cours de sensibilisation en ligne, d'exercices sur l'hameçonnage, de formation à la politique de sécurité et de formations précises en fonction des rôles (par exemple, formation au traitement des incidents ou à la continuité des activités).

2. **Élaborez des politiques et des protocoles critiques en matière de cybersécurité.** Le simple fait d'avoir une politique ne garantit pas la mise en place d'activités appropriées. Il vous faut des protocoles qui garantissent le respect des protocoles. Tous les employés doivent connaître les politiques et être capables de suivre les protocoles dont ils sont responsables. Vous devriez disposer d'une politique de sécurité globale avec des responsabilités organisationnelles et des politiques ou protocoles spécifiques pour les exigences clés en matière de cybersécurité, comme les contrôles d'accès, la gestion des correctifs et la réponse aux incidents.

3 **Établissez un alignement interne sur les exigences en matière de cybersécurités**. La position par défaut de nombreuses organisations est que la cybersécurité est un « problème de TI ». Il y a plusieurs raisons à cela. Cependant, la cybersécurité est plutôt un problème opérationnel pour les municipalités. Par conséquent, il doit y avoir un bon alignement interne sur les priorités municipales et la façon dont la cybersécurité protège les renseignements et les systèmes qui soutiennent la municipalité. Un bon moyen d'y parvenir est de s'assurer que le gouvernement et les professionnels techniques s'entendent. Il s'agit également de sensibiliser les dirigeants et les administrateurs municipaux à la cybersécurité en tant que préoccupation municipale.

4 **Gérez les risques liés aux tiers**. La plupart des petites et moyennes organisations n'ont pas besoin d'une infrastructure des TI. L'utilisation de services de tiers présente plusieurs avantages pratiques et économiques, notamment le passage au « nuage » et l'utilisation de la « sécurité en tant que service ». Voici quelques éléments clés à prendre en compte :

- Examinez minutieusement les fournisseurs pour comprendre ce qu'ils offrent par rapport à vos besoins en cybersécurité – assurez-vous de bien comprendre vos besoins et de les documenter.
- Incluez le fournisseur tiers dans votre planification de la cybersécurité.
- Comprenez les risques liés aux tiers – ceux qu'ils peuvent poser et ceux que vous leur demandez de contribuer à atténuer.
- Mettez en place des communications claires et établissez et assurez un lien de confiance sur la base des dispositions contractuelles avec le fournisseur – préservation des renseignements, contrôles de cybersécurité… ne faites pas de suppositions. N'utilisez pas de contrats types.
- Indiquez toute relation entre la prestation de services de tiers et l'assurance.

Communications et planification de l'état de préparation

1 **Dressez une liste des personnes qui doivent participer à la gestion d'une cyberattaque.** Assurez-vous d'avoir leurs coordonnées.

Cette liste devrait inclure les membres suivants :

- Décideurs;
- Équipes de communication;
- Équipes juridiques (et éventuellement un fournisseur externe de cyberassurance);
- Experts techniques;
- Direction du fournisseur;
- Responsables des relations avec les fournisseurs.

2 **Organisez un exercice de planification pour le meilleur et le pire des scénarios.**

- Déterminez les intervenants qui pourraient être touchés.

- Évaluez les processus et les transactions pour déterminer lesquels sont les plus critiques et élaborez des procédures pour les exécuter manuellement. Si possible, formez le personnel à ces processus manuels.
- Déterminez les fournisseurs qui devront être mobilisés.

3 **Si possible, nommez une seule personne qui gérera la communication en cas de crise.** Celle-ci sera chargée de veiller à ce que chaque membre de votre municipalité soit en mesure de livrer un message cohérent aux intervenants.

4 **Déterminez à quel moment les gestionnaires de première ligne doivent envoyer les problèmes à un échelon supérieur.**

- Y a-t-il ou risque-t-il d'y avoir des dommages pour la santé ou les biens?
- Y a-t-il des preuves d'un acte criminel ou d'un autre acte répréhensible?
- Y a-t-il un intérêt public considérable?
- Le problème touche-t-il une partie critique la mission de nos activités?
- Des erreurs ou des fautes ont-elles été commises dans la réponse de l'organisation?

5 **Définissez un protocole pour déterminer qui doit être informé des problèmes et à quel moment.**

- N'oubliez pas que vos ordinateurs pourraient être inaccessibles dans le pire des scénarios. Assurez-vous que toutes les coordonnées sont conservées sur papier. Indiquez plusieurs moyens de contact pour chaque personne figurant sur la liste : téléphone fixe, téléphone cellulaire, adresse courriel qui ne dépend pas de l'infrastructure municipale, et tout autre point de contact tel qu'un téléphone de chalet.
- Établissez un lieu physique où l'équipe pourra se réunir en personne pendant une crise.
- Déterminez quels types d'aide professionnelle externe peuvent être nécessaires.
- Incluez dans la liste les hauts responsables politiques, les autorités chargées de l'application de la loi et le personnel provincial comme le Commissariat à la protection de la vie privée.
- Planifiez les messages à l'intention des intervenants internes. Les intervenants internes se verront poser des questions concernant toute cyberintrusion et devraient être en mesure de répondre aux préoccupations des électeurs.

6 Effectuez une analyse des intervenants**. N'oubliez pas que vos intervenants se parleront entre eux. Veillez donc à ce que les renseignements que vous fournissez soient cohérents.** Pour chaque grand public, identifiez et définissez :

- Le principal gestionnaire des relations;
- Ce que vous voulez que cet intervenant fasse;
- Les principaux messages que vous communiquerez à cet intervenant;
- Vos outils, vos chaînes et votre déploiement de communication.

Gestion des incidents

1. **Ayez un plan**. En vous référant à votre évaluation des menaces et des risques, sachez où se trouvent vos renseignements critiques, établissez des valeurs relatives aux renseignements qui vous aideront à évaluer le niveau et l'urgence de votre réponse. Il existe de nombreuses ressources en ligne et la page *Contrôles de cybersécurité de base pour les petites et moyennes organisations* du Centre canadien pour la cybersécurité est un bon point de départ, tout comme d'autres ressources sur la cybersécurité destinées aux organisations de taille comparable.

2. **Créez des stratégies**. La stratégie soutient le plan et établit les processus de gestion des incidents de votre organisation, ainsi que les rôles et responsabilités clés. Cela comprend les listes de personnes-ressources, les dispositions et les responsabilités des tiers, ainsi que des conseils sur le signalement et la gestion des dossiers pendant un incident.

3. **Mettez le plan à l'épreuve**. Vous ne saurez jamais si le plan fonctionnera si vous ne le mettez pas à l'épreuve. Vous devez le faire régulièrement. Une bonne façon de mettre le plan à l'épreuve est de procéder à des exercices sur table – il s'agit d'un moyen efficace de gérer et de pratiquer des scénarios applicables avec les personnes de votre organisation qui ont des responsabilités en matière de réponse aux incidents.

4. **Améliorez le plan**. Votre organisation évolue et les menaces aussi. Passez régulièrement le plan en revue, pratiquez-le et prenez des mesures pour l'améliorer afin que votre organisation soit prête à réagir rapidement face à un incident de cybersécurité.

Communications

Il est essentiel que la nouvelle de l'intrusion soit communiquée aux intervenants clés par vous-même et non par une fuite. Il est tout aussi important de ne pas en dire plus que nécessaire ou de ne pas faire de déclarations qui pourraient envenimer la situation.

1. **Élaborez rapidement des déclarations des faits sommaires.** Ces déclarations constituent une réponse que les porte-parole et le personnel de la municipalité peuvent fournir au public, à la presse et aux autres intervenants pendant que l'intrusion fait l'objet d'une enquête et que vous déterminez les mesures à prendre. Elles vous accorderont le temps nécessaire pour que vous puissiez déterminer les prochaines étapes. Voici un exemple de déclaration des faits sommaire :

MODÈLE DE DÉCLARATION DE DETENTION :

« Nous enquêtons actuellement sur un cyberincident potentiel ayant touché nos systèmes municipaux. À l'heure actuelle, rien ne prouve que des données personnelles identifiables ont été consultées, mais les enquêtes se poursuivent. Nous avons verrouillé tous les systèmes concernés pour éviter tout autre incident et travaillons avec nos partenaires des technologies de l'information pour résoudre l'incident. Nous avons prévenu les autorités chargées de l'application de la loi et nous coopérerons pleinement à leur enquête. »

2. **Ne spéculez pase**. Ne dites rien de plus que ce que vous savez ou ne donnez pas de fausses assurances – il est normal de dire que l'incident est toujours en cours d'analyse. Ces déclarations ne doivent pas contenir d'hypothèses incorrectes qui peuvent nuire à la crédibilité plus tard. Les équipes juridiques et les autorités chargées de l'application de la loi doivent être consultées au fur et à mesure de l'élaboration de ces déclarations afin de s'assurer que vous n'augmentez pas votre vulnérabilité juridique ou que vous ne fournissez pas d'informations utiles aux criminels.

3. **Veillez à décrire l'incident dans un langage précis.** Consultez vos experts quant au langage approprié pour décrire l'incident. Par exemple, vous ne devez pas décrire l'incident comme une violation de données, sauf si vous avez confirmé qu'il y a eu un accès non autorisé ou une perte de données. Vous éviterez ainsi de fournir des renseignements erronés ou de faire des déclarations qui pourraient être utilisées contre vous plus tard.

4. **Maintenez un dialogue permanent avec les intervenants.** Dans la mesure du possible, communiquez avec eux plutôt que d'attendre qu'ils vous contactent. Cela renforcera votre crédibilité et leur donnera l'assurance que vous intervenez de manière appropriée.

   Les communications internes doivent avoir lieu en premier, dans la mesure du possible. Cela :

   - Permet aux dirigeants de diriger;
   - Renforce la confiance des employés.

5. **Donnez à vos employés des réponses aux questions types afin qu'ils sachent comment répondre aux préoccupations des intervenants.**

6. **Un message cohérent crée des alliés.** Vos intervenants veulent que vous réussissiez à contenir l'attaque et à protéger votre municipalité.

Questions juridiques et risques

Sachez que votre exposition à tout incident comprendra une exposition potentielle à une intervention réglementaire ou à un litige. En plus de votre exposition à l'incident lui-même, vous pourriez être exposé à d'autres risques selon la façon dont vous gérez votre réponse. Il est recommandé de faire appel à un conseiller juridique pour limiter les risques.

Le conseiller juridique peut aider avec :

- La gestion de la réponse à l'intrusion;
- La préservation des preuves;
- Les conseils sur les implications juridiques de votre réponse, y compris la stratégie de communication, la production de rapports, les notifications et les risques de litige;
- L'identification des tiers touchés.

Préservation du privilège

Il est important de veiller à ce que certaines catégories d'investigations informatiques restent juridiquement privilégiées afin d'éviter tout risque de litige.

- Il est peu probable que les communications concernant la source de l'attaque et les mesures correctives soient couvertes par le privilège juridique.
- L'investigation informatique concernant l'étendue de la compromission potentielle, ou les zones de défense qui pourraient être renforcées, peut être protégée.
- Les communications avec des tiers ne resteront privilégiées que tant que les deux parties partagent un intérêt commun. Le privilège sera perdu s'il est probable qu'une action en justice soit intentée entre les parties, ou si des déclarations jetant le blâme sur quelqu'un (p. ex. un fournisseur) sont faites.

Obligations en matière de déclaration et de notification

En général, si des données personnelles peuvent avoir été touchées, un rapport au Commissariat à la protection de la vie privée et une notification aux personnes touchées doivent être faits dès que possible.

D'autres notifications peuvent être exigées par la loi ou recommandées pour atténuer les risques. Il peut s'agir de notifier les employés touchés, les organisations financières (en particulier si des renseignements bancaires ou de cartes de crédit ont pu être compromis) et la police.

Coopération avec les autorités chargées de l'application de la loi Premières étapes

1. **La sécurité est la priorité absolue.** S'il existe un risque pour la sécurité des personnes, il faut d'abord prendre des mesures pour les en protéger ou les en avertir.

2. **Si la sécurité n'est pas une préoccupation ou si elle a été gérée, agissez de façon à protéger vos systèmes et vos données.**

   - Isolez les systèmes infectés – voire l'ensemble du réseau – d'Internet et des connexions de tiers, si possible, sauf dans ces cas :
   - Si l'accès non autorisé est en cours, il peut être utile de surveiller cette activité pour recueillir des preuves concernant les motifs, les techniques et l'attribution

3. **Si le système d'origine peut être identifié, une capture de la mémoire vive ou la suspension d'un service de machine virtuelle touchée facilitera l'analyse et l'enquête.**

4. **Dans la mesure du possible, préservez les preuves numériques, y compris :**

   - Les fichiers journaux;
   - Les captures d'écran de tout message ou activité inhabituelle;
   - Les fichiers et processus suspects et malveillants (Sysinternals);
   - Les comptes d'utilisateurs inconnus ou nouvellement créés;
   - L'activité sur des adresses IP suspectes;
   - Les notes de rançon;
   - Les sobriquets/adresses électroniques;
   - Les adresses de sites Tor;
   - Les ID des portefeuilles BTC;
   - Toute communication avec l'acteur de la menace.

Signalement des cybercrimes à la police

Si vous avez des raisons de croire qu'un crime a été commis, signalez l'incident à la police dès que possible. Le fait d'impliquer la police dans la situation pendant l'enquête lui permettra de vous aider à prendre les mesures appropriées pour protéger vos résidents et enquêter sur le crime.

De nombreux cybercrimes ne sont pas signalés, car les victimes craignent que l'incident ne devienne public ou que la police n'entrave la réponse à l'attaque. Cette attitude accroît le risque de cyberattaque, car les criminels pensent qu'ils peuvent éviter tout risque de poursuites pour leurs actes.

Voici quelques exemples de cybercriminalité :

- Accès non autorisé aux systèmes, comme des violations de données, du piratage, du vol de données et une prise de contrôle de comptes de messagerie et de médias sociaux.
- Méfait sur les données, y compris leur altération, leur suppression ou leur mise hors d'usage d'une quelconque autre façon.
- Attaque de services Web, par des attaques par déni de service, des défigurations de pages Web, des injections SQL, des scripts de site à site, des falsifications de requêtes de site à site et d'autres méthodes.
- Utilisation de logiciels malveillants.

Pendant l'enquête

Les autorités chargées de l'application de la loi travailleront avec les administrateurs des TI et les entreprises de sécurité tierces pour identifier les attaquants et recueillir des preuves numériques.

Les enquêteurs devront s'entretenir avec votre personnel pour recueillir des renseignements sur l'incident et recueillir des preuves numériques. Ils comprendront qu'une réponse peut être en cours et travailleront avec vous pour éviter d'y nuire.

- Les entretiens durent environ 1 à 2 heures par personne.
- Des questionnaires peuvent être fournis pour être remplis à l'avance.

En tant que cible, vous devez vous concentrer sur ce qui suit :

- Arrêter l'attaque et prévenir toute autre exposition;
- Systèmes de nettoyage;
- Mettre en place des mesures de sécurité;
- Reprendre les activités normales;
- Communications, tant externes qu'internes.

Préservation des preuves

La préservation des preuves doit être orientée par la source de l'intrusion et l'étendue de la compromission.

- Il est nécessaire de comprendre la source de l'intrusion pour pouvoir résoudre les brèches en matière de sécurité.
- Comprendre l'étendue de la compromission déterminera les obligations en matière de déclaration et de notification que vous pourriez avoir et permettra au conseiller de vous éclairer sur la stratégie de réduction des risques.

Les équipes des TI peuvent détruire accidentellement des preuves dans leurs efforts visant à contenir l'intrusion et éliminer l'intrus. Les conseils d'un avocat ou d'un policier peuvent s'avérer essentiels pour gérer la réponse à l'intrusion de manière à préserver les preuves qui pourraient être nécessaires pour déterminer l'étendue de l'intrusion et pour soutenir de futures poursuites intentées.

Conclusion

Malheureusement, aucun ensemble de meilleures pratiques ou de mesures de cybersécurité ne mettra votre municipalité à l'abri d'une attaque potentielle. Toutefois, en veillant à ce que votre municipalité fasse l'effort de mettre en place des contrôles appropriés et élabore un plan de réponse en cas d'attaque, vous réduisez le risque d'être attaqué et la gravité de tout cyberincident.

Annexe A

Auteurs de contenu

Ruth Promislow, Bennett Jones LLP

Bob Gordon, CCTX

Randy Purse, CD, PhD, CTDP

Ashley Lukeeram, CISSP, CEH, CRISC, Tenable

Tyson Johnson, CyberNB

John Douglas, Douglas Communications Group

Eldon Sprickerhoff, eSentire Inc.

Imran Bashir, KPMG

Paul Sammut, KPMG

John Weigelt, Microsoft

DS Vern Crowley, OPP

Ben Smith, RSA

Et un remerciement spécial au Groupe consultatif sur la cybersécurité de l'industrie pour leur contribution.

TECHNATION^CA

Financé en partie
par le gouvernement
du Canada

Canada