SAINT-CYPRIEN

POLITIQUE DE GESTION DES INCIDENTS DE SÉCURITÉ INFORMATIQUE

AVRIL 2024

PROVINCE DE QUÉBEC

MUNICIPALITÉ DE SAINT-CYPRIEN

MRC DES ETCHEMINS

POLITIQUE DE GESTION DES INCIDENTS DE SÉCURITÉ INFORMATIQUE

SÉANCE ordinaire du conseil municipal de la Municipalité de Saint-Cyprien, tenue le 9 avril 2024, à 19h00, à la salle du conseil municipal au 399, rue Principale, à laquelle étaient présents :

LE MAIRE, M. Michel Bernard

LES MEMBRES DU CONSEIL :

- M. Gilles Audet
- Mme Réjeanne Gosselin
- M. Édouard Fournier
- M. Charles Therrien
- Mme Joane Rochon
- M. Michael Mercier

Tous les membres du conseil formant un quorum.

CONSIDÉRANT QUE la Municipalité de Saint-Cyprien (ci-après la « Municipalité ») est un organisme public assujetti à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c. A -2.1 (ci-après la « Loi sur l'accès »);

CONSIDÉRANT QUE la Municipalité s'engage à protéger les renseignements personnels qu'elle collecte et traite dans le cadre de ses activités dans le respect des lois et règlements applicables;

EN CONSÉQUENCE, LE CONSEIL DÉCRÈTE CE QUI SUIT :

OBJECTIF

La sécurité informatique est au cœur de notre organisation. Face à la multiplication des menaces, il est impératif de disposer d'une stratégie claire et efficace pour répondre aux incidents de sécurité. Cette politique vise à assurer une réponse rapide, coordonnée et efficace à tout incident de sécurité, minimisant ainsi les impacts négatifs et garantissant la continuité des opérations.

DÉFINITIONS

Événement : Toute occurrence observable dans un système ou réseau. Cela peut être aussi simple qu'un utilisateur se connectant à un service ou qu'un serveur répondant à une demande.

Incident de sécurité informatique : Violation ou menace imminente de violation des politiques de sécurité informatique, des règles d'utilisation ou des standards de sécurité. Cela peut inclure des tentatives d'accès non autorisées, des malwares ou toute autre activité malveillante.

POLITIQUE

1. Réponse aux incidents de sécurité informatique

La direction de notre municipalité joue un rôle primordial dans la gestion des incidents de sécurité informatique. Elle s'engage fermement à soutenir toutes les initiatives en matière de réponse aux incidents, garantissant ainsi que les ressources nécessaires sont toujours disponibles. L'objectif principal de cette politique est de clarifier son but, qui est centré sur la protection de nos actifs informatiques tout en minimisant les perturbations potentielles. Cette politique couvre spécifiquement nos systèmes, réseaux et données. Pour assurer une compréhension homogène, nous avons défini clairement les termes clés utilisés dans cette politique.

En ce qui concerne la structure organisationnelle, nous avons mis en place des directives claires sur les responsabilités de chaque membre de l'équipe en cas d'incident. Cela comprend la définition des rôles, des responsabilités et des niveaux d'autorité. De plus, pour une gestion efficace, nous avons classé les incidents selon leur gravité, ce qui nous permet d'apporter une réponse appropriée en fonction de la situation.

L'évaluation de notre réponse aux incidents est cruciale. Par conséquent, nous avons intégré des mesures de performance pour évaluer régulièrement l'efficacité de nos interventions. Enfin, la communication étant un élément essentiel en cas d'incident, nous avons établi des canaux de communication clairs, définissant comment et quand communiquer, que ce soit en interne ou avec des parties externes.

2. Plan de Réponse

Notre réponse aux incidents définit notre raison d'être et tracent nos aspirations à long terme dans la gestion des incidents et la protection des renseignements personnels et confidentiels que nous détenons. Ces éléments guident nos actions et nous rappellent constamment pourquoi une gestion efficace des incidents est cruciale pour la municipalité. Pour concrétiser cette mission et cette vision, nous avons établi des stratégies claires et des objectifs précis, définissant non seulement ce que nous souhaitons accomplir, mais aussi comment nous comptons y parvenir.

Il est essentiel que notre plan bénéficie du soutien total de notre direction. C'est pourquoi nous nous sommes assurés que notre plan de réponse aux incidents est approuvé par les plus hauts niveaux de la municipalité, garantissant ainsi son alignement avec nos objectifs globaux. En ce qui concerne la structure organisationnelle, nous avons soigneusement défini comment notre équipe de réponse aux incidents est structurée, veillant à ce qu'elle soit parfaitement intégrée dans l'organisation.

La communication est au cœur de notre plan. Nous avons mis en place des protocoles spécifiques pour informer efficacement les parties prenantes internes et le public en cas d'incident. Cette transparence renforce la confiance et assure que toutes les parties concernées sont correctement informées. Pour garantir que nous restons sur la bonne voie, nous utilisons des méthodes spécifiques pour évaluer régulièrement l'efficacité de notre réponse aux incidents. Enfin, notre approche de la réponse aux incidents n'est pas isolée ; elle s'intègre harmonieusement dans nos opérations globales, assurant une cohérence et une coordination à tous les niveaux de l'organisation.

PROCÉDURES DE RÉPONSE

Des procédures détaillées, basées sur la politique et le plan, couvrant toutes les étapes de la réponse aux incidents, de la détection à la résolution ont été élaborées dans le but de bien encadrer la marche à suivre.

1. Détection

- **Surveillance continue :** Utilisez des outils de surveillance et des logiciels de détection d'intrusion pour surveiller en permanence le trafic réseau et l'activité des systèmes.
- **Alertes :** Configurez des alertes pour signaler toute activité suspecte ou non conforme.
- **Journalisation :** Assurez-vous que tous les systèmes et applications conservent des journaux détaillés pour faciliter l'analyse post-incident.
- **Revue régulière :** Effectuez des contrôles réguliers pour identifier les signes d'incidents potentiels.

2. Identification

- **Analyse :** Évaluer l'alerte ou le rapport pour déterminer s'il s'agit d'un véritable incident de sécurité.
- **Classification :** Catégoriser l'incident en fonction de sa gravité et de son impact potentiel.
- **Documentation :** Documenter tous les détails pertinents de l'incident pour référence future.

3. Endiguement (Containment en anglais)

- **Endiguement à court terme :** Prendre des mesures immédiates pour limiter l'impact de l'incident, comme déconnecter un système compromis du réseau.
- **Analyse en profondeur :** Examiner l'incident pour comprendre sa portée et son origine.
- **Endiguement à long terme :** Mettre en place des mesures pour empêcher la récurrence de l'incident pendant que la cause profonde est traitée.

4. Éradication

- Recherche de la cause profonde : Identifier la cause sous-jacente de l'incident.
- **Suppression :** Éliminer la cause profonde de l'incident, que ce soit un logiciel malveillant, une vulnérabilité non corrigée, etc.

5. Récupération

- **Restauration et validation :** Restaurer les systèmes à leur état normal et valider qu'ils sont sains.
- **Surveillance renforcée :** Surveiller étroitement les systèmes pour s'assurer qu'il n'y a pas de signes de réapparition de l'incident.

6. Leçons apprises

- **Réunion de rétrospective :** Rassembler toutes les parties impliquées pour discuter de ce qui s'est bien passé, de ce qui aurait pu être fait différemment, et de comment prévenir des incidents similaires à l'avenir.
- **Mise à jour de la documentation :** Mettre à jour tous les documents pertinents, y compris la politique, le plan et les procédures, en fonction des leçons apprises.
- **Formation et sensibilisation :** Organiser des sessions de formation pour sensibiliser davantage le personnel aux menaces actuelles et aux meilleures pratiques pour les prévenir.

7. Communication

- **Notification interne :** Informer la direction et les parties prenantes concernées de l'incident, de son impact et des mesures prises.
- **Notification externe :** Si nécessaire, informer les clients, les partenaires ou le public de l'incident, surtout si des données personnelles ont été compromises.
- **Coordination avec les autorités :** En cas d'incident grave, collaborer avec les autorités locales ou nationales pour enquêter et résoudre l'incident.

Communication avec des Tiers

Établissement de protocoles pour la communication avec des tiers, en coordination avec les relations publiques, le département juridique et la direction.

ÉQUIPE DE RÉPONSE AUX INCIDENTS

Modèles d'équipe

- **Équipe centrale :** Une équipe unique, généralement basée au siège, qui gère tous les incidents.
- **Équipes distribuées :** Plusieurs équipes réparties géographiquement, chacune gérant des incidents dans une zone spécifique.
- **Équipe de coordination :** Une équipe centrale qui coordonne la réponse entre plusieurs équipes distribuées.
- **Responsable de la protection des renseignements personnels :** Cette personne doit toujours être impliquée dans ce processus.

Sélection du modèle

Choix basé sur la disponibilité, le coût, l'expertise et la culture organisationnelle.

Composition de l'équipe

Des membres qualifiés, dotés de compétences techniques avancées et d'aptitudes à la communication.

Collaboration Interdépartementale

Identification et coordination avec d'autres départements essentiels : juridique, relations publiques, ressources humaines, continuité des activités, sécurité physique.

Services complémentaires

- **Détection d'intrusion :** Surveillance proactive des systèmes pour détecter toute activité suspecte.
- **Diffusion d'alertes :** Informer l'organisation des nouvelles menaces et vulnérabilités.
- **Éducation et sensibilisation :** Former le personnel à la sécurité et aux meilleures pratiques.
- **Partage d'informations :** Échanger des informations sur les incidents avec d'autres organisations pour améliorer la posture de sécurité globale.

RECOMMANDATIONS FINALES

- **Mise en place d'une capacité formelle de réponse :** Assurer que la municipalité est prête à répondre à tout moment.
- **Élaboration et mise à jour régulière de la politique, du plan et des procédures :** Garantir que les procédures sont toujours pertinentes.
- **Formation continue de l'équipe :** Assurer que l'équipe est toujours à jour avec les dernières menaces et technologies.

RÉVISION DE LA POLITIQUE

La sécurité de nos systèmes et données est primordiale. Cette politique est un outil essentiel pour garantir une réponse efficace en cas d'incident, protégeant ainsi l'intégrité de notre organisation et la confiance de nos partenaires et clients.

Cette politique doit être régulièrement révisée et mise à jour pour s'assurer qu'elle reflète les meilleures pratiques actuelles et répond aux menaces émergentes.

ENTRÉE EN VIGUEUR

La présente politique entre en vigueur dès son adoption par le conseil.

Copie certifiée conforme à Saint-Cyprien, le 16 avril 2024.

Stéphanie Asselin

_____

Stéphanie Asselin
Directrice générale et greffière-trésorière

Michel Bernard

_____

Michel Bernard
Maire

Adoption de la politique : 9 avril 2024
Avis de promulgation : 16 avril 2024