Ordre des géologues du Québec

Politique de réponse aux cyberincidents

Adoptée le 10 décembre 2024

Table des matières

1. Préambule

Face à l'évolution constante des cybermenaces, un plan d'intervention est essentiel pour réagir efficacement aux cyberincidents. En période de crise, l'incertitude peut compromettre une réponse appropriée. Un plan structuré permet de gérer la situation de manière organisée, réduisant ainsi le risque d'oublier des aspects critiques et limitant l'impact sur l'organisation.

2. Objectif

Le but de cette politique est de s’assurer que l’organisation est prête à intervenir en cas de cyberincident de manière à pouvoir reprendre rapidement ses activités minimisant ainsi les impacts sur les opérations, la confidentialité, l'intégrité et la disponibilité des informations.

3. Portée

La portée de cette procédure inclut tous les réseaux, systèmes et données, ainsi que les parties prenantes (p. ex. : clients, partenaires, employés, sous-traitants, fournisseurs tiers) qui accèdent à ces réseaux, systèmes et données. Elle couvre tous les incidents de sécurité informatique, y compris, mais sans s'y limiter, les violations de données, les attaques par déni de service (DDoS), les logiciels malveillants, et les tentatives d'intrusion.

4. Définition

Un incident de cybersécurité peut ne pas être reconnu ou détecté immédiatement.

Un cyberincident est tout événement susceptible de compromettre la confidentialité, l'intégrité, ou la disponibilité des systèmes informatiques, des réseaux ou des données de l'organisation. Certains indicateurs peuvent être les signes d’une atteinte à la sécurité, qu’un système a été compromis, d’une activité non autorisée, etc. Il faut toujours être à l’affût de tout signe indiquant qu'un incident de sécurité s'est produit ou est en cours.

Certains de ces indicateurs sont décrits ci-dessous :

1. Activité excessive ou inhabituelle de la connexion et du système, notamment à partir de tout identifiant d'utilisateur (compte d'utilisateur) inactif.
2. Accès distant excessif ou inhabituel dans votre organisation. Cela peut concerner le personnel ou des fournisseurs tiers.
3. L'apparition de tout nouveau réseau sans fil (Wi-Fi) visible ou accessible.
4. Une activité inhabituelle liée à la présence de logiciels malveillants, de fichiers suspects ou programmes exécutables nouveaux ou non approuvés.

5. Ordinateurs, lecteurs de disque dur ou autres supports média perdus, volés ou égarés qui contiennent des données de cartes de paiement, renseignements personnels ou d'autres données sensibles.

5. Type d'incidents

Type d'incidents	Description
Accès ou utilisation non autorisés	Un individu obtient un accès physique ou logique au réseau, au système ou aux données sans autorisation.
Interruption ou déni de service	Attaque qui empêche l'accès au service ou compromet son fonctionnement normal.
Programme malveillant	Installation d'un maliciel (p. ex. : virus, ver, cheval de Troie ou autre code).
Rançongiciel	Type spécifique de programme malveillant qui infecte un ordinateur et affiche des messages demandant le paiement d'une somme d'argent en contrepartie du rétablissement du système.
Déni de service distribué (DDoS)	Les attaques par déni de service distribué visent les sites Web et les services en ligne. L'objectif est de submerger ces sites et services d'un trafic supérieur à ce que le serveur ou le réseau peut traiter. L'objectif est de rendre le site Web ou le service inopérant. Parmi les symptômes, on retrouve des échecs de connexion généralisés ou des erreurs de non-disponibilité du système.
Défaillances du système de réseau (généralisées)	Incidents compromettant la confidentialité, l'intégrité ou la disponibilité des réseaux.
Défaillances du système d'application	Incidents compromettant la confidentialité, l'intégrité ou la disponibilité des applications ou des systèmes.
Divulgation non autorisée ou perte d'informations	Incident compromettant la confidentialité, l'intégrité ou la disponibilité des données.
Atteinte à la vie privée	Incident qui implique une perte réelle ou supposée de renseignements personnels.
Atteinte à la protection des données/sécurité de l'information	Incident qui implique une perte réelle ou supposée d'informations sensibles.
Compromission des données de comptes	Atteinte à la protection des données des cartes de paiement. Ce type d'incident entraîne un accès non autorisé aux données des cartes de paiement (données du titulaire de la carte ou données d'authentification sensibles) ou l'exposition de ces données.
Autres	Tout autre incident qui affecte les réseaux, les systèmes ou les données.

6. Responsabilités et coordonnées des personnes-ressources

Équipe de Réponse aux Incidents (ERI) : Un groupe dédié qui prend en charge la détection, la réponse, et la résolution des incidents. Cette équipe est responsable de la gestion de bout en bout du cyberincident.

Direction : Assure une supervision stratégique et prend les décisions critiques concernant l'escalade, les communications externes et les relations avec les autorités.

Utilisateurs : Tout utilisateur du réseau ou des systèmes de l'organisation doit signaler immédiatement tout incident ou comportement suspect à l'ERI.

Rôle	Nom	Téléphone	Adresse de courriel
Direction et responsable du traitement des incidents	Jean-François Bouchard	(514) 278- 6220	dirgen@ogq.qc.ca
Responsable des TI	Nexxo Technologies	(514) 548-3466	support@nexxo.tech
Responsable des TI	Connexence	(418) 380-5815	info@connexence.com
Assureur en cybersécurité	BFL Canada	(514) 843-3632	digitalsupport@bflcanada.ca

7. Description des procédures

a) Préparation à la gestion des incidents

En préparation d'un incident de cybersécurité, il faut :

- Créer une copie électronique et une copie papier du plan d'intervention en cas d'incident.
- La copie papier du plan est conservée dans un endroit connu et accessible.
- Effectuer un examen et une mise à jour annuels du plan d'intervention en cas d'incident.
- Assurer la mise sur pied d'une équipe d'intervention en cas d'incident de cybersécurité.

    - Dédié, virtuel, ou disponible.
    - Dispenser la formation nécessaire.
- Documenter les rôles et responsabilités.
    - Délégation de pouvoirs.
    - Dispenser la formation nécessaire.
- Effectuer régulièrement des exercices.
    - Tester le plan, l'équipe et les outils.
- Comprendre l'environnement.
    - Schémas, emplacement des systèmes et des données critiques.
    - Assurer une visibilité des réseaux et des systèmes pour intervenir en cas d'incident.
    - Environnement du fournisseur.
    - Comprendre les dépendances.
- Comprendre les mesures de contrôle mises en place.
    - Sont-elles suffisantes pour atténuer le risque à un niveau acceptable?
- Comprendre les impacts.
    - Déterminer le temps d'interruption maximal tolérable et acceptable (durée pendant laquelle une activité peut être interrompue sans préjudice important et pendant laquelle un système peut être indisponible).
    - Liste hiérarchisée des actifs et des temps d'interruption.
- Préparer la cellule de crise.
    - Déterminer et préparer un lieu de réunion, physique ou numérique.
    - S'assurer que le lieu est sécurisé et équipé de manière appropriée.
- Établir à l'avance un plan de communication.
- S'assurer qu'un point de contact centralisé est mis à la disposition des employés pour signaler les incidents de cybersécurité réels ou présumés.
- S'assurer que tous les employés savent qu'ils sont tenus de signaler les événements de cybersécurité et comment le faire.
- Sensibilisation et formation continue des utilisateurs à la sécurité informatique.

b) Lorsqu'un incident est identifié

Lorsqu'un incident de cybersécurité est détecté, il faut :

- Réunir les personnes qui sont au courant de l'incident.
- Aviser l'équipe d'intervention en cas d'incident de cybersécurité.
- Rappeler à tous ceux qui sont responsables de toujours s'en tenir aux faits.
    - Sinon, le temps n'est consacré qu'à la gestion de la désinformation.
- Communiquer de manière efficace et efficiente.
- Se réunir dans la cellule de crise.
    - S'assurer que le lieu est sécurisé et équipé de manière appropriée.
- Déterminer la source de vulnérabilité et mettre en œuvre les correctifs nécessaires.
- Examiner les informations et les mesures prises à ce jour.
- Signaler l'incident au personnel interne approprié et aux entreprises externes.
- Éradiquer l'incident.

- S'assurer que les appareils mis en danger sont formatés avant d'être remis en service.
    - S'assurer que les preuves nécessaires ont été recueillies.
- Veiller à ce que l'incident ne puisse pas se reproduire.
- Mieux comprendre la méthode utilisée pour l'attaque et les vulnérabilités exploitées.

c) Atteinte à la protection des données – Intervention spécifique

S'il a été confirmé qu'un incident de sécurité lié à une atteinte à la protection des données s'est produit, il faudra effectuer les étapes supplémentaires suivantes :

- Compléter le registre d'incidents de confidentialité pour documenter l'incident.
- Examiner l'atteinte à la protection des données pour déterminer si des **renseignements personnels** ont été perdus en raison d'un accès non autorisé ou d'une divulgation non autorisée et qu'il existe un risque de préjudice sérieux pour les personnes concernées.
    - Dans un tel cas, le signaler à la Commission de l'accès à l'information (CAI) au Québec ou au Commissaire à la protection de la vie privée du Canada.

d) Rançongiciel – Intervention spécifique

S'il a été confirmé qu'un incident de sécurité de rançongiciel s'est produit, il faudra effectuer les étapes supplémentaires suivantes :

- Déconnecter immédiatement du réseau les appareils visés par un rançongiciel.
- Examiner le rançongiciel et déterminer comment il a infecté l'appareil. Cela vous aidera à comprendre comment l'éliminer.
- Communiquer avec les autorités locales pour signaler l'incident et coopérer à leur enquête.
- Une fois le rançongiciel supprimé, une analyse complète du système doit être effectuée à l'aide d'un antivirus, d'un anti-maliciel et de tout autre logiciel de sécurité le plus récent disponible afin de confirmer qu'il a été supprimé de l'appareil.
- Si le rançongiciel ne peut pas être supprimé de l'appareil (souvent le cas avec les programmes malveillants furtifs), l'appareil doit être réinitialisé au moyen des supports ou des images d'installation d'origine.
    - Avant de procéder à la réinitialisation à partir de supports de sauvegarde, vérifier que les supports/images de sauvegarde ne sont pas infectés par des maliciels.
- Si les données sont critiques et doivent être restaurées, mais ne peuvent être récupérées à partir de sauvegardes non affectées, rechercher les outils de décryptage disponibles sur **nomoreransom.org**.
- Ne pas payer la rançon, sous réserve des circonstances et des enjeux en cause.
- Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des rustines pour empêcher toute nouvelle attaque.

e) Piratage de compte – Intervention spécifique

S'il a été confirmé qu'un piratage de compte s'est produit, il faudra effectuer les étapes supplémentaires suivantes :

- Vérifier si on a encore accès au compte en ligne.
  - Sinon, communiquer avec le support pour tenter de récupérer l'accès.
- Changer le mot de passe utilisé pour se connecter à la plateforme.
- Si le mot de passe est réutilisé ailleurs, changer également tous ces mots de passe.
- Activer le double facteur d'authentification pour la plateforme.
- Supprimer les connexions et les appareils non légitimes de l'historique de connexion.

f) Perte ou vol d'un appareil – Intervention spécifique

S'il a été confirmé qu'une perte d'équipement s'est produite, il faudra effectuer les étapes supplémentaires suivantes :

- Le vol ou la perte d'un bien, tel qu'un ordinateur, un ordinateur portatif ou un appareil mobile, doit être signalé immédiatement aux autorités policières locales. Cela inclut les pertes/vols en dehors des heures d'ouverture normale et pendant les week-ends.
- Si l'appareil perdu ou volé contenait des données sensibles et qu'il n'est pas crypté, effectuer une analyse de sensibilité, du type et du volume des données volées, y compris les numéros de cartes de paiement potentiellement concernés.
- Dans la mesure du possible, verrouiller/désactiver les appareils mobiles perdus ou volés (p. ex. : téléphones intelligents, tablettes, ordinateurs portatifs, etc.) et procéder à un effacement des données à distance.

g) Reprise à la suite de l'incident

Pour un retour à la normal à la suite de l'incident de cybersécurité, il faut :

- Remettre progressivement les systèmes touchés dans un état de disponibilité.
- Assurer une surveillance rigoureuse pour s'assurer que l'incident ne se reproduit pas et qu'il n'est pas encore en cours.
- Veiller à ce que les systèmes soient restaurés à partir d'une source fiable.
- Confirmer le fonctionnement normal des systèmes touchés.
- Mettre en place une surveillance supplémentaire pour rechercher de futures activités.
- Au besoin, communiquer avec l'assureur pour soumettre une demande d'indemnisation.
- Tenir une réunion pour discuter des leçons apprises dans un délai de 2 semaines.

- Produire un rapport de suivi.
- Consulter et examiner le compte rendu d'incident.
  - Comment l'incident a-t-il été détecté, par qui et quand?
  - Portée et gravité de l'incident.
  - Méthodes utilisées pour le confinement et l'éradication.
- Recenser des possibilités d'amélioration pour être mieux préparé.
- Assurer la responsabilité du suivi des occasions d'amélioration identifiées.

8. Communication et notification

Communication interne : Toute information pertinente liée à un cyber incident doit être partagée avec les parties prenantes concernées, incluant le CAGR et la direction.

Notification externe : Selon la gravité de l'incident et les exigences légales, les parties externes, telles que les régulateurs ou les clients, doivent être informées dans les délais requis.

Rapport aux autorités : Si nécessaire, l'incident doit être signalé aux organismes chargés de la cybersécurité ou aux autorités judiciaires.

9. Confidentialité et sensibilité

Les informations relatives aux cyber incidents doivent être traitées avec le plus haut niveau de confidentialité pour protéger la réputation de l'organisation et se conformer aux réglementations en vigueur.

10. Révision et mise à jour

Cette politique sera révisée régulièrement (au moins une fois par an) pour s'assurer qu'elle reste en phase avec l'évolution des menaces et des technologies de cybersécurité.

11. Historique des versions

Numéro de version	Date de révision	Description des modifications	Auteurs des modifications
1.0	10 décembre 2024	Version initiale	Rédaction : Alain Cromp Révision : Charlotte Athurion