FONDATIONS COMMUNAUTAIRES DU CANADA | Institut de formation

FICHE OUTIL - Fondations communautaires du Canada CYBERSÉCURITÉ ET CONFIDENTIALITÉ

18 juillet 2024

De nos jours, nous sommes submergés par une mer de données. Malheureusement, nous ne les gérons pas toujours de façon idéale, et c'est peu de le dire. Or, les organismes à but non lucratif, comme toute autre organisation ou entreprise, recueillent plus d'informations que jamais, et c'est certainement plus qu'ils ne savent en gérer.

Nous traitons des renseignements personnels et financiers au quotidien. Ce faisant, nous (et nos clients) courons des risques, parfois même sans le savoir. Une chose est sûre : lorsqu'on parle de gérer et de stocker des données en toute sécurité, la prévoyance est de mise.

Tous les organismes à but non lucratif doivent collecter des données pour assurer leur efficacité et leur succès. Il va sans dire que ces informations peuvent parfois être très sensibles. Votre fondation communautaire a le mandat de protéger les données que vous avez recueillies, mais souvent, cette responsabilité n'est pleinement comprise qu'une fois que le mal est fait.

Quelles sont les zones de danger?

Où stockez-vous les données que vous collectez? Habituellement, ces données sont stockées dans des classeurs, sur des serveurs réseau ou dans une infrastructure infonuagique. Cependant, si elles échappent à votre contrôle, vous pourriez vous attirer des ennuis. Voici quelques zones de danger qui concernent les organismes à but non lucratif exerçant leurs activités en ligne et hors ligne :

- **Hameçonnage et ingénierie sociale** – manipulation dans le but d'obtenir des informations confidentielles;
- **Rançongiciel** - logiciel malveillant qui crypte les données et demande une rançon pour les récupérer;
- **Menaces internes** - violation de données de la part des employés ou des bénévoles (par inadvertance ou par malveillance);
- **Menaces persistantes avancées (APT)** - cyber-attaques prolongées et ciblées visant à voler des données.stockage de renseignements personnels sur des serveurs ou des

systèmes infonuagiques, ou à des sites physiques non sécurisés (par exemple, des classeurs déverrouillés);
- **Attaques *Zero-Day*** - attaques exploitant des vulnérabilités inconnues dans les logiciels.

Vos obligations en cas de violation de données

Une tentative de piratage peut avoir de graves conséquences, et c'est aussi le cas pour la perte ou la destruction de données. Les ordinateurs portables et les téléphones intelligents comportant des données sensibles peuvent être perdus, endommagés ou même volés, ce qui peut faire tomber vos données entre de mauvaises mains. Connaissez-vous vos obligations à cet égard?

Le Conseil des normes de sécurité PCI a promulgué la norme de sécurité des données de l'industrie des cartes de paiement, qui oblige les organisations à suivre les « pratiques exemplaires en matière de sécurité de l'information » si elles gèrent des cartes figurant parmi les principales cartes de crédit, telles que Visa et Mastercard. Les organisations qui ne respectent pas ces normes peuvent être sanctionnées et devoir payer des amendes considérables.

Il existe d'autres réglementations sur la sécurité des données au Canada, telles que la Loi sur la protection des renseignements personnels sur la santé de l'Ontario, que votre organisme à but non lucratif doit respecter si vous traitez des renseignements sur la santé qui sont protégés. Il faut savoir que ces règlements sont susceptibles de changer; il est donc important de vous tenir au fait des dernières mises à jour. Consultez l'annexe A pour obtenir des liens et des renseignements sur la législation provinciale à propos de la protection des renseignements personnels.

Renseignements permettant d'identifier une personne

Quels renseignements permettent d'identifier une personne? La définition peut varier d'une province à l'autre, mais en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), les renseignements personnels comprennent tout renseignement factuel ou subjectif, enregistré ou non, au sujet d'une personne identifiable. Cela comprend toutes sortes d'informations, dont :

- l'âge, le nom, les numéros d'identification, le revenu, l'origine ethnique ou le groupe sanguin;
- les opinions, les évaluations, les commentaires, le statut social ou les mesures disciplinaires;
- les dossiers des employés, les dossiers de crédit, les dossiers de prêt, les dossiers médicaux, l'existence d'un différend entre un consommateur et un commerçant, les intentions (par exemple, acquérir des biens ou des services, ou changer d'emploi).

D'après la LPRPDE : « Les organisations visées par la LPRPDE doivent habituellement obtenir le consentement des personnes lorsqu'elles recueillent, utilisent ou communiquent des renseignements personnels les concernant. Les personnes ont le droit de consulter les renseignements personnels que détient une organisation à leur sujet. Elles ont aussi le droit d'en contester l'exactitude. Les renseignements personnels ne peuvent être utilisés qu'aux fins auxquelles ils ont été recueillis. L'organisation qui entend les utiliser à d'autres fins doit, de nouveau, obtenir le consentement de le faire. Les renseignements personnels doivent être protégés par des mesures appropriées. »

Mesures à mettre en place

Savez-vous quoi faire en cas de violation de données? Savez-vous qui appeler en premier? Vous devez disposer d'un plan spécifique à votre fondation communautaire. Celui-ci doit présenter les procédures, lister les personnes à contacter et recenser toutes les coordonnées pertinentes.

De nos jours, les entreprises doivent également disposer d'une assurance contre les cyberrisques. Cette dernière aurait pu être perçue comme un « luxe » autrefois, mais elle est désormais devenue une nécessité. Qui plus est, le coût des primes de telles assurances n'est rien comparé aux honoraires exigés par un avocat en cas de violation de données. Un des bons côtés de postuler (oui, postuler) pour obtenir ce type d'assurance est que vous devrez revoir vos mesures de sécurité actuelles. Il s'agit d'une excellente occasion d'améliorer la sécurité de vos points faibles. Votre organisme doit être couvert non seulement contre les pertes qu'il pourrait subir, mais aussi contre les réclamations résultant de pertes subies par des tiers, comme des donateurs ou des clients. Parmi les coûts que vous pourriez devoir assumer figurent :

- la responsabilité liée au contenu;
- la responsabilité liée à la violation de données;
- les dépenses liées à une enquête réglementaire;
- la gestion de crise;
- les dépenses liées aux notifications.

Gérez les données avec soin

Nous devons prêter une plus grande attention à la façon dont nous transférons les données entre les espaces de stockage et les appareils. La loi énonce que les sociétés et les entreprises doivent protéger ces données, quel que soit l'endroit où elles sont stockées : documentation papier, réseaux informatiques, appareils mobiles, appareils personnels ou systèmes autonomes. Dans ce contexte, la « sécurité des données » peut être définie comme « leur confidentialité, leur

intégrité et leur disponibilité ». La protection des renseignements personnels, cependant, concerne « l'utilisation appropriée des données ».

Que pouvez-vous faire pour veiller encore davantage à la sécurité des données que vous gérez? Vous pouvez utiliser des pratiques exemplaires, qui existent depuis longtemps.

- Assurez-vous d'avoir un programme de gestion des correctifs en place pour protéger la technologie que vous utilisez. Ces mises à jour de sécurité constituent une excellente première ligne de défense.
- Utilisez un cryptage robuste. Verrouillez les disques durs des ordinateurs portables et veillez à la sécurité de tous les appareils mobiles au moyen de codes d'accès et de réseaux virtuels privés (*VPN* en anglais), qui sont un groupe d'ordinateurs mis en réseau sur un réseau public (par exemple, sur Internet). De plus, cryptez les données sensibles. Si possible, ne stockez pas de renseignements permettant d'identifier une personne sur des appareils mobiles.
- Prévoyez des séances de formation régulières pour vos employés. Développez une culture de la sécurité afin que les employés se soucient réellement des données au lieu de se contenter de visionner une vidéo une fois par année.
- Mettez sur pied une politique « Prenez vos appareils personnels » (PAP, ou *BYOD* [en anglais]). Si les employés sont autorisés à utiliser leurs propres appareils, établissez des directives claires concernant l'accès aux renseignements personnels et l'autorisation de les consulter.

Évaluez le degré de préparation de votre entreprise face aux cyberrisques

Il est essentiel que les fondations communautaires prennent des mesures proactives dans ce domaine. Il leur faut au moins :

- concevoir un plan de réponse aux incidents;
- souscrire une assurance contre les cyberrisques;
- créer un plan de continuité des activités dans le cadre d'un exercice visant à amener le personnel et le conseil d'administration à réfléchir aux mesures de rétablissement après incident, aux impératifs opérationnels, etc.

Lors de l'élaboration de leurs plans de cybersécurité, les fondations doivent trouver un équilibre entre les risques, les mesures raisonnables, les ressources, la capacité et les coûts.

La Vancouver Foundation a accompli beaucoup de travail dans ce domaine. Pour ce faire, elle a répondu à un sondage de dix questions pour l'aider à concevoir son plan.

1. **Mettre en place des contrôles d'accès solides**
   - Authentification multifactorielle (MFA) : Exigez l'authentification multifactorielle pour tous les comptes afin d'ajouter une couche supplémentaire de sécurité.
   - Principe du moindre privilège : Accordez aux utilisateurs l'accès minimum nécessaire à l'accomplissement de leurs tâches.

2. **Mettre régulièrement à jour et corriger les systèmes**
   - Mises à jour automatisées : Veillez à ce que les systèmes et les applications soient configurés pour être mis à jour automatiquement.
   - Gestion des correctifs : Appliquez régulièrement des correctifs pour corriger les vulnérabilités connues.

3. **Organiser régulièrement des formations à la sécurité**
   - Simulations d'hameçonnage : Organisez périodiquement des simulations d'hameçonnage pour apprendre aux employés à reconnaître les menaces.
   - Programmes de sensibilisation à la sécurité : Mettez en œuvre des programmes de formation continue sur les meilleures pratiques en matière de sécurité.

4. **Utiliser des outils de détection des menaces avancées**
   - Détection et réponse des points finaux (EDR) : Déployez des solutions EDR pour surveiller les menaces et y répondre.
   - Renseignements sur les menaces : Utilisez les services de renseignement sur les menaces pour rester informé des menaces émergentes.

5. **Élaborer et tester des plans de réponse aux incidents**
   - Équipe d'intervention en cas d'incident (IRT) : Mettez en place une équipe de réaction aux incidents (IRT) avec des rôles et des responsabilités clairement définis.
   - Exercices réguliers : Organisez régulièrement des exercices d'intervention en cas d'incident afin de garantir la préparation.

6. **Assurer le cryptage des données**
   - Données au repos et en transit : Cryptez des données sensibles pour les protéger contre les accès non autorisés.
   - Chiffrement de bout en bout : Mettez en œuvre un chiffrement de bout en bout pour les communications et les transferts de données.

7. **Effectuer des évaluations régulières de la sécurité**
   - Analyse des vulnérabilités : Recherchez régulièrement des vulnérabilités dans votre réseau et vos applications.
   - Tests d'intrusion : Effectuez des tests d'intrusion périodiques afin d'identifier et de corriger les faiblesses en matière de sécurité.

8. **Sécuriser les interactions avec les tiers**
    - Gestion des risques liés aux fournisseurs : Évaluez le niveau de sécurité des fournisseurs tiers et exigez d'eux qu'ils se conforment à vos normes de sécurité.
    - Contrôles d'accès des tiers : Limitez et surveillez l'accès des tiers à vos systèmes et à vos données.

9. **Élaborez des plans de sauvegarde et de rétablissement**
    - Sauvegardes régulières : Effectuez des sauvegardes régulières des données critiques et vérifiez leur intégrité.
    - Plan de récupération post-incident : Élaborez et testez un plan de reprise après sinistre pour assurer la continuité de l'activité.

10. **Surveiller les menaces et y répondre**
    - Centre d'opérations de sécurité (SOC) : Mettez en place un SOC pour surveiller, détecter et répondre aux incidents de sécurité.
    - Surveillance continue : Utilisez des outils de surveillance continue pour détecter les anomalies et les menaces potentielles en temps réel.

Concevez un plan de réponse aux incidents

D'après les experts en cybersécurité, la question n'est pas de savoir *si* votre organisation sera victime d'une cyberattaque, mais plutôt *quand*. Un plan complet de réponse aux incidents de cybersécurité est nécessaire pour que vous puissiez vous fier à une ligne directrice solide lorsque l'inévitable se produit. Tout plan doit aborder les éléments suivants :

1. identification des incidents – détection et définition de la menace;
2. mesures appropriées – confinement et éradication;
3. rétablissement des systèmes;
4. rapports et suivi.

De nombreuses ressources sont accessibles gratuitement aux professionnels de l'informatique. Elles définissent l'ensemble des étapes à suivre pour favoriser l'adoption de pratiques exemplaires en matière de cybersécurité et de plans de réponse aux incidents. Le cadre adopté par la Vancouver Foundation s'appuie fortement sur le travail de CREST, un organisme d'accréditation en cybersécurité à but non lucratif basé au Royaume-Uni. Le plan de cette fondation est décrit à l'annexe B. Voici un lien vers une autre ressource pour l'élaboration d'un tel plan : How to Create a Nonprofit Cyber Incident Response Plan.

Respectez la loi à la lettre

Bien que les lois canadiennes sur la protection des renseignements personnels n'énoncent aucune règle interdisant d'utiliser un environnement infonuagique, l'ARC exige que certains dossiers soient conservés au Canada. S'il est bien géré, le stockage infonuagique est une option sécurisée pour la plupart des organismes à but non lucratif.

En ce qui concerne la confidentialité et le stockage des données, il est également important de savoir en quoi les règles adoptées aux États-Unis et en Europe diffèrent de celles du Canada. Depuis 2015, date de la fin de l'accord du *Safe Harbor* entre les États-Unis et l'Europe, de nouvelles dispositions sont mises en place concernant les données et la confidentialité, et celles-ci auront des incidences à l'échelle mondiale.

Il existe d'excellentes options de stockage infonuagiques sécurisées. Consultez vos collègues des fondations communautaires pour connaître les options qu'ils utilisent.

De quelle façon travaillez-vous avec des tiers (par exemple, des fournisseurs)? Stipulez vos conditions dans vos contrats. Il est raisonnable de s'attendre à ce que vos fournisseurs aient une couverture contre les erreurs et les omissions pour vous protéger. Discutez ouvertement de la responsabilité que le fournisseur est prêt à assumer et de la manière dont il le fera.

Lignes directrices relatives à la politique de protection de la vie privée

Il est essentiel de disposer d'une politique claire et complète en matière de protection de la vie privée. Veillez à ce que votre politique comprenne

Partage d'informations et la confidentialité

- Association of Fundraising Professionals Code: Adhérer à des lignes directrices telles que : « Les membres doivent adhérer au principe selon lequel toutes les informations sur les donateurs et les prospects créées par ou au nom d'une organisation ou d'un client sont la propriété de cette organisation ou de ce client et ne doivent pas être transférées ou utilisées sauf au nom de cette organisation ou de ce client.

Déclarations de principe

- Déclaration de protection de la vie privée : Inclure une déclaration selon laquelle l'organisation protège la vie privée des administrés en préservant la confidentialité de toutes les informations les concernant.

- Protocoles de diffusion de l'information : Préciser comment et quand les informations seront divulguées, telles que les adresses, les numéros de téléphone et les adresses électroniques.

- Demandes de tiers : Définir le processus de gestion des demandes d'information émanant de tiers et préciser ce que le personnel est autorisé à dire.

S'adapter à la croissance des données

Alors que les données continuent de croître de manière exponentielle, les organisations à but non lucratif doivent s'adapter pour mieux les gérer et être prêtes à faire les choses différemment. La sauvegarde des données doit être aussi prioritaire que les causes servies.

Ressources

Une bonne ressource à considérer est le *Key Policy Template Manual* de FCC, qui comprend un exemple de politique de confidentialité et de protection de la vie privée.

Pour en savoir plus :

- Canadian privacy law, cloud computing and how it applies to nonprofits
- A Nonprofit's Cyber Liability And Data Privacy
- Data Privacy and Cyber Liability: What You Don't Know Puts Your Mission at Risk
- Innovating Canada: Cybersecurity
- Supporting Your Secure Cloud Journey with 4 Questions
- How Remote Workforces Change the Way we Approach Digital Security

Nous remercions TechSoup de nous avoir donné l'autorisation de réimprimer des extraits du billet de blogue invité intitulé « Privacy and Data Concerns for Nonprofits » par Cheryl Biswas, consultante en matière de menaces informatiques (18 mai 2016).

ANNEXE A : LÉGISLATION PROVINCIALE SUR LA CONFIDENTIALITÉ

Certaines provinces n'ont pas de législation dans ce domaine. Les provinces suivantes ont adopté leurs propres lois à cet égard.

ALBERTA : Personal Information Protection Act (PIPA)
Cette loi concerne la protection des renseignements personnels dans le secteur privé de l'Alberta et comprend des règlements sur la façon dont les organisations recueillent, utilisent et divulguent les renseignements personnels de leurs employés.
https://www.alberta.ca/personal-employee-information.aspx

COLOMBIE-BRITANNIQUE : Personal Information Protection Act (PIPA)
En vertu de cette loi, les particuliers ont le droit d'accéder à leurs renseignements personnels. La loi énonce également les dispositions selon lesquelles les organisations peuvent collecter, utiliser et divulguer des informations personnelles.
https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information

NOUVELLE-ÉCOSSE: Personal Information International Disclosure Protection Act (PIIDPA)
Cette loi limite le stockage et l'accès aux informations personnelles du gouvernement de la Nouvelle-Écosse à l'extérieur du Canada.
https://novascotia.ca/just/iap/piidpaquest.asp#:~:text=PIIDPA%20makes%20it%20illegal%20for,Canada%2C%20unless%20certain%20circumstances%20exist

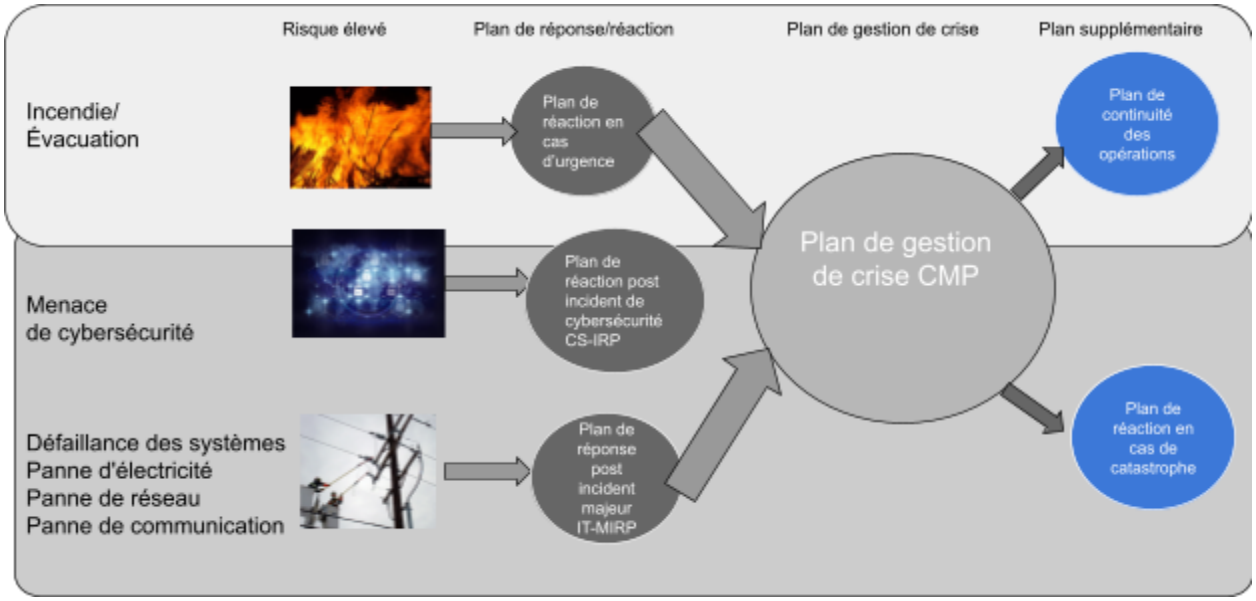
QUÉBEC : Loi sur la protection des renseignements personnels dans le secteur privé
Cette loi s'adresse aux employeurs du secteur privé et réglemente la protection des renseignements personnels qu'un employeur recueille, détient, utilise ou communique à des tiers dans le cadre de ses activités.
http://legisquebec.gouv.qc.ca/fr/showdoc/cs/P-39.1

NUNAVUT : Access to Information and Protection of Privacy Act (ATIPP)
Donne aux individus le droit d'accéder aux informations détenues par les organismes publics et établit des protections de la vie privée.
https://www.gov.nu.ca/sites/default/files/documents/2024-02/atipp_manual_-_part_1.pdf

Annexe B : Plan de réponse aux cyberattaques de la Vancouver Foundation

Cadre:

Le plan de réponse cybernétique de la VF est un sous-ensemble d'une série de dangers à haut risque et de plans spécifiques aux dangers qui ont plongé dans un plan de gestion de crise (CMP), un plan de continuité des activités (BCP) et un plan de réponse en cas de catastrophe (DRP).



Identifier les incidents – détecter et définir la menace :

Lorsqu'il est question de cybersécurité, en particulier dans les cas de vol de propriété intellectuelle, il est fréquent que les intrusions passent inaperçues dans le système pendant un certain temps avant d'être détectées. L'identification d'un incident de cybersécurité présumé (par exemple, la surveillance d'événements inhabituels et l'évaluation d'un ou plusieurs points de déclenchement) a été intégrée aux fonctions opérationnelles de la Vancouver Foundation. Les examens de routine des journaux de pare-feu et les mécanismes d'alerte de port anormal font partie du tissu de sécurité du pare-feu Fortinet utilisé à la Fondation. De plus, la direction demande au personnel de la Vancouver Foundation de signaler tout comportement inhabituel sur le réseau, tout courriel provenant d'expéditeurs suspects ou inconnus, ainsi que les lacunes relatives à l'information et la perte de service, et fait des rappels fréquents à cet effet. Tous les signalements sont rapportés à un point central, à savoir le service d'assistance. Le personnel est

invité à noter tous les détails importants (par exemple, le type de violation, les messages à l'écran et d'autres détails sur l'événement inhabituel), ce qui aide les techniciens lors du rétablissement après incident, de l'analyse des causes profondes, et lors d'éventuelles activités de litige en aval.

Comprendre l'attaque :

Une fois qu'un incident de cybersécurité a été identifié, le personnel informatique définit ensuite les objectifs de la réponse, en répondant à des questions telles que :

- Comment l'incident a-t-il été détecté?
- Qui a signalé l'incident et quand?
- Quels sont les premiers indicateurs de compromission (IOC)?
- Quelles mesures ont été prises immédiatement après la détection?
- Quels sont les systèmes, les applications et les données touchés?
- Quelle est l'étendue de la compromission (par exemple, nombre de systèmes, type de données touchés)?
- L'incident est-il isolé ou généralisé à l'ensemble du réseau?
- Quelles sont les conséquences possibles sur les opérations commerciales et la sécurité des données?
- De quel type de cyberattaque s'agit-il (par exemple, logiciel malveillant, rançongiciel, hameçonnage, DDoS)?
- Qui pourrait être responsable de l'attaque (menace interne, pirate informatique externe, État-nation)?
- Quels sont les vecteurs d'attaque et les méthodes utilisées (par exemple, courrier électronique, application web, intrusion dans le réseau)?

Déterminer quelles informations ont été divulguées à des parties non autorisées, volées, supprimées ou corrompues est un résultat clé à ce stade et sera réalisé rapidement et de manière cohérente.

Effectuer le triage – classer et hiérarchiser les incidents :

Bien que chaque situation soit différente, le personnel informatique est encouragé à catégoriser l'intrusion au moyen d'une matrice, comme la suivante par exemple :

Categorie	Description	Type d'événement
Critique	**Incidents causant des dommages ou des perturbations graves, entraînant un impact opérationnel important ou une perte de données, et nécessitant une**	**Attaque par rançongiciel cryptant les données critiques de l'entreprise, violation majeure des données sensibles des clients, attaque DDoS perturbant tous les services.**

	réponse immédiate et complète.	
Important	**Incidents ayant un impact considérable sur les opérations ou les données, pouvant entraîner de graves perturbations et nécessitant une réponse rapide et ciblée.**	**Attaque par hameçonnage ciblé compromettant les informations d'identification des employés clés, infection par des logiciels malveillants sur plusieurs postes de travail, accès non autorisé à des systèmes non critiques.**
Mineur	**Incidents ayant un impact limité sur les opérations ou les données, causant une perturbation minimale et nécessitant des procédures d'intervention routinières.**	**Infection par un logiciel malveillant d'un seul utilisateur contenue par l'antivirus, tentative mineure d'hameçonnage sur du personnel non critique, tentative d'accès non autorisé à petite échelle sans perte de données.**
Peu important	**Incidents ayant un impact négligeable, nécessitant principalement une surveillance et des mesures de précaution standard.**	**Courriels indésirables sans lien d'hameçonnage, tentatives infructueuses d'intrusion, activités à faible risque.**

Mesures prises par les « répondants de première ligne » :

En plus d'IT Ideas, la Vancouver Foundation entretient des relations étroites avec des fournisseurs experts en cybersécurité, notamment Mirai Security et le conseiller juridique Norton Rose Fullbright.

Savoir quand transmettre un cas à l'échelon supérieur et faire appel à des ressources plus spécialisées est un aspect important de l'analyse initiale, et cela permet de veiller à ce que les informations clés soient captées. Parmi les données clés figurent la date et l'heure, l'adresse IP, le port (source ou destination) et le système (matériel ou fournisseur, système d'exploitation, application, etc.). Dans le cadre du plan plus large de continuité des activités et de réponse aux incidents de la Vancouver Foundation, le présent document décrit des canaux de signalement clairs et des points de transmission à l'échelon supérieur[1].

---

[1] Remarque : Le *plan de continuité des activités et de réponse aux incidents* d'Acredo Consulting a été rédigé et publié en octobre 2018.

	Description	Exemple
Entrées pare-feu	Enregistrements de tout le trafic réseau entrant et sortant à travers le pare-feu	Entrées de journal indiquant les tentatives d'accès non autorisé bloquées
Entrées système	Entrées de journal des systèmes d'exploitation détaillant les événements et les activités du système	Enregistrements des connexions des utilisateurs, des redémarrages du système et des erreurs
Entrées applications	Entrées de journal enregistrant l'utilisation des applications et les erreurs	Entrées de journal indiquant les pannes d'application ou les activités inhabituelles
Entrées intrusions système	Enregistrements des intrusions potentielles détectées	Entrées de journal montrant la détection d'une activité réseau suspecte
Entrées accès	Enregistrements de l'accès des utilisateurs aux systèmes et aux données	Entrées de journal indiquant les heures et les lieux de connexion des utilisateurs
Entrées courriel	Entrées de journal des courriels envoyés et reçus, y compris les pièces jointes	Entrées de journal indiquant les pièces jointes suspectes ou les tentatives d'hameçonnage
Entrées authentification	Enregistrements des tentatives d'authentification et de leurs résultats	Entrées de journal indiquant les échecs et les réussites des tentatives de connexion
Entrées journal	Entrées de journal des requêtes, des mises à jour et des tentatives d'accès aux bases de données	Entrées de journal indiquant les tentatives d'accès non autorisé aux données
Entrées point de terminaison	Entrées de journal des dispositifs d'extrémité, y compris les journaux des logiciels antivirus et de sécurité	Entrées de journal indiquant la détection de logiciels malveillants sur les postes de travail

Contenir l'incident de cybersécurité

Une fois que l'enquête initiale a été effectuée et qu'une intrusion réelle a été reconnue, l'équipe limitera les dommages causés par l'incident de cybersécurité en l'empêchant de se propager à d'autres réseaux et appareils, tant au sein de l'organisation qu'à l'extérieur de celle-ci. Les activités de confinement comprennent :

- bloquer (et consigner) les accès non autorisés;

- bloquer les sources de logiciels malveillants (par exemple, les adresses courriel et les sites Web);
- fermer les ports et les serveurs de messagerie spécifiques;
- modifier les mots de passe de l'administrateur système lorsqu'un cas de corruption est présumé;
- procéder au filtrage au moyen d'un pare-feu;
- déplacer les pages d'accueil du site Web;
- isoler les systèmes;
- conserver les preuves ainsi que la documentation sur les mesures prises (captures de données, archives des journaux de pare-feu, etc.) si une action en justice est requise plus tard dans le processus.

Éradiquer la cause de l'incident

Il faut mettre ces mesures en œuvre avec rapidité et précision. Une fois qu'un incident a été maîtrisé, il est souvent nécessaire d'éliminer les composants clés de l'incident, ainsi que d'identifier et d'atténuer les vulnérabilités qui ont été exploitées. Au cours de ce processus d'éradication, les actions que le service informatique entreprendra comprennent :

- identifier tous les hôtes touchés au sein (et parfois au-delà) de l'organisme, afin de corriger la situation;
- réaliser l'analyse de logiciels malveillants;
- enquêter sur toute réponse de l'attaquant aux mesures prises par le service informatique;
- concevoir une réponse (de préférence à l'avance) si l'attaquant utilise une méthode d'attaque différente;
- permettre suffisamment de temps pour s'assurer que le réseau est sécurisé et que l'attaquant ne persiste pas.

Réunir et conserver les preuves

Les preuves seront recueillies à divers moments de l'enquête. L'ensemble des éléments de preuve sera régi par deux règles principales, à savoir :

- admissibilité de la preuve – détermine si la preuve peut ou non être utilisée devant un tribunal;
- poids de la preuve – la qualité et l'exhaustivité des preuves.

Communiquer avec le conseiller juridique de la Fondation (Fasken LLP) ainsi qu'avec des experts en cybersécurité (Mirai Security) est important à ce stade-ci. À cette fin, il est essentiel que la Vancouver Foundation conserve la chaîne de possession à la fois sur papier et sous forme

électronique. Une façon d'y parvenir est de tenir un journal écrit détaillé de chaque action au cours de l'enquête afin que :

- l'on puisse se référer à des preuves claires et précises à une date ultérieure, et que des experts de l'opposition puissent répéter la séquence des événements et des mesures prises, si nécessaire.

Ce journal des actions comprendra :

- les informations d'identification (par exemple, l'emplacement, le numéro de série, le numéro de modèle, le nom d'hôte, les adresses MAC et les adresses IP d'un ordinateur);
- le nom, le titre et le numéro de téléphone de chaque personne qui a recueilli ou traité les preuves au cours de l'enquête;
- l'heure et la date (y compris le fuseau horaire) de chaque moment où les preuves ont été traitées;
- les emplacements où les preuves ont été stockées.

Rétablir les systèmes, les données ou la connectivité

La dernière étape de la réponse à un incident de cybersécurité consiste à rétablir le fonctionnement normal des systèmes, à confirmer que les systèmes fonctionnent normalement et à corriger les vulnérabilités pour éviter que des incidents similaires ne se produisent. Il va sans dire que la reconnexion des réseaux, la reconstruction des systèmes et la restauration, la recréation ou la correction des informations prennent du temps. L'entreprise doit donc établir les priorités de rétablissement informatique après incident et comprendre la nécessité de suivre ces étapes de manière approfondie. Les plans de rétablissement après incident appropriés comprennent les points suivants :

- la reconstruction des systèmes infectés (souvent à partir de sources « propres » connues);
- le remplacement des fichiers corrompus par des versions propres, ou leur restauration;
- la suppression des contraintes temporaires imposées pendant la période de confinement;
- la réinitialisation des mots de passe sur les comptes corrompus;
- l'installation de correctifs, la modification des mots de passe et le renforcement de la sécurité du périmètre réseau, par exemple, les ensembles de règles de pare-feu;
- des essais approfondis des systèmes, y compris des contrôles de sécurité;
- la confirmation de l'intégrité des systèmes et des mesures de contrôle de l'entreprise.

Il est important de vérifier que les systèmes fonctionnent à nouveau normalement, par exemple au moyen d'un essai d'intrusion indépendant des systèmes concernés, en plus d'une évaluation

des contrôles de sécurité. L'équipe remettra des rapports sur les efforts d'éradication, en précisant que ces étapes ont été réalisées avec succès et en notant toutes les exceptions et autres conclusions importantes. Elle sera suivie d'une explication plus approfondie des activités qui ont eu lieu.

Rapports et suivi

Les recherches dans ce domaine soulignent l'importance d'accorder du temps aux activités de suivi à la suite d'un incident de cybersécurité.

Les principaux intervenants aideront le service informatique en s'assurant de réserver des ressources suffisantes pour mener ces efforts à bien et en reportant d'autres priorités pendant les étapes importantes :

- mener une enquête suffisante pour identifier le ou les auteurs du crime;
- identifier et analyser les causes profondes;
- évaluer l'incidence commerciale de l'incident;
- fournir le soutien nécessaire aux enquêtes criminelles;
- effectuer l'analyse des tendances.

Une fois qu'un incident de cybersécurité a été traité avec succès, un rapport formel sera produit pour les parties prenantes internes et externes. Les questions clés à prendre en compte varient selon la nature de l'intrusion, mais comprennent notamment les suivantes :

- Quelles sont les exigences de la Fondation en matière de rapports, et à quelles entités constitutives doivent-ils être faits?
- Que dois-je signaler?
- Sous quel format dois-je signaler l'incident?
- Quel est l'objectif du signalement?

Enfin, une description complète de la nature de l'incident, de son historique et des mesures prises pour rétablir la situation après l'incident est requise. Celle-ci doit comprendre :

- une estimation réaliste des répercussions financières attribuables à l'incident et des autres conséquences sur l'entreprise (atteinte à la réputation, perte de contrôle de gestion, croissance freinée, etc.);
- des recommandations concernant les contrôles améliorés ou supplémentaires nécessaires pour prévenir, détecter et corriger les incidents de cybersécurité, ou pour faciliter la reprise après les éventuels incidents.

Réaliser un bilan après incident

Examiner et améliorer les procédures d'intervention, partager les enseignements tirés et mettre à jour les documents et les contrôles pertinents. L'examen porte notamment sur la qualité des prestations du personnel, les informations nécessaires et les mesures correctives.

Les questions auxquelles il faut répondre lors d'un tel examen peuvent inclure les suivantes :

1. Dans quelle mesure le personnel et la direction ont-ils bien géré l'incident? Les procédures documentées ont-elles été suivies? Étaient-elles adéquates?
2. De quelles informations aurions-nous eu besoin plus tôt?
3. Des mesures ou des actions qui auraient pu entraver le rétablissement après incident ont-elles été prises?
4. Des événements imprévus auraient-ils pu être évités?
5. Que feraient le personnel et la direction différemment si un incident de cybersécurité similaire se produisait?
6. Comment la communication des renseignements à d'autres organismes aurait-elle pu être améliorée?
7. Quelles mesures correctives pourraient empêcher des incidents similaires à l'avenir?
8. Quels signes précurseurs ou indicateurs faut-il surveiller pour détecter des incidents similaires?
9. Comment les résultats peuvent-ils être utilisés dans la méthodologie d'évaluation des risques de la Vancouver Foundation?
10. Quelles leçons avons-nous apprises?

Communiquer les apprentissages réalisés et les consolider

La communication avec toutes les parties prenantes doit être claire, concise et axée sur la résolution des problèmes et l'amélioration des mesures de contrôle. Un plan d'action sera ensuite créé pour expliquer comment l'organisation consolidera les enseignements tirés de l'incident pour devenir plus résiliente face aux futures attaques de cybersécurité.

Mettre à jour les informations, contrôles et documents clés

À la suite d'un incident de cybersécurité, il est important de mettre à jour les approches de réponse aux incidents de cybersécurité, les contrôles et les documents associés.