Guide sur les rançongiciels

ITSM.00.099

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

Vue d'ensemble

Un rançongiciel est un type de maliciel qui empêche une utilisatrice ou un utilisateur légitime d'accéder à des ressources (système ou données) jusqu'à ce qu'il verse une rançon. Cette situation peut avoir un effet dévastateur sur les organisations et les particuliers. Les organisations risquent de perdre l'accès à leurs données et à leurs dispositifs essentiels, ce qui les empêcherait de mener leurs activités ou de servir la clientèle.

Nous avons constaté une recrudescence des attaques par rançongiciel touchant autant des organisations canadiennes que des particuliers. L'Évaluation des cybermenaces nationales 2025-2026 (ECMN) précise que les rançongiciels constituent la principale menace émanant de la cybercriminalité à laquelle font face les secteurs des infrastructures essentielles du Canada. Les rançongiciels perturbent directement la capacité des entités des infrastructures essentielles à offrir des services critiques, ce qui peut nuire au bien-être physique et émotionnel des victimes. Au cours des deux prochaines années, les auteurs de menace menant des attaques par rançongiciel demeureront une menace importante pour le Canada.

Les auteurs de menace ont adapté leurs tactiques de façon à forcer les organisations victimes à payer une rançon en menaçant de divulguer les données ou les justificatifs d'authentification volés dans le but d'humilier publiquement l'organisation ciblée. Selon l'ECMN, les auteurs d'attaques par rançongiciel continueront très probablement à utiliser les avancées de l'intelligence artificielle (IA) et de la cryptomonnaie pour développer de nouvelles tactiques d'extorsion lucratives. Les incidents liés aux rançongiciels sont devenus de plus en plus sophistiqués, ciblés et complexes. Il devient également de plus en plus difficile pour une organisation de se défendre contre ces attaques et de s'en remettre, plus particulièrement si elle possède peu de ressources pour faire face à la situation.

Les tactiques opérationnelles des auteurs de menace se font également plus discrètes. Elles impliquent l'accès aux systèmes de communication d'une organisation pour repérer les systèmes essentiels et les données de grande importance qui pourraient causer une atteinte à la réputation si ces données étaient divulguées. Les auteurs de menace déploient ensuite le rançongiciel aux jeux de données et aux systèmes les plus importants ou ayant la plus grande valeur, compromettant ainsi l'organisation. De plus, les auteurs de menace surveillent étroitement les communications et les mesures de reprise prévues de l'organisation pour miner ses efforts et infiltrer davantage les réseaux et les dispositifs connectés.

Les renseignements contenus dans la présente publication visent à informer les organisations et à les aider à réduire les risques d'attaques par rançongiciel, à atténuer les conséquences de ces

attaques et à prendre des mesures préventives pour les contrer. Ils peuvent également aider les organisations à définir leurs exigences opérationnelles et de sécurité, ainsi qu'à mettre en œuvre des politiques et procédures pertinentes relatives à la cybercriminalité.

La présente publication traite des rançongiciels, des motivations et gains des auteurs de menace, de même que des mesures à prendre pour empêcher ces attaques et protéger votre organisation. La publication se divise en trois sections :

- **Découvrir les rançongiciels :** Cette section vise à définir un rançongiciel et à exposer les vecteurs communs utilisés pour infecter les réseaux et les dispositifs.
- **Se défendre contre les cybermenaces :** Cette section vise à fournir une liste de mesures préventives pour protéger votre organisation et à offrir des listes de vérification pour certaines mesures d'atténuation précises. Lorsque vous appliquez ces mesures, vous disposez de meilleures pratiques exemplaires en cybersécurité et d'une protection accrue contre les cyberincidents et les auteurs de menace, y compris les rançongiciels.
- **Se remettre d'un incident lié à un rançongiciel :** Cette section donne des indications sur les mesures immédiates à prendre dès la découverte d'un rançongiciel, sur les mesures de reprise et sur les méthodes nécessaires pour évaluer l'incident et renforcer les mesures de sécurité. En suivant les recommandations dans cette section, les organisations pourront réagir efficacement à un incident et réduire le risque de devenir victimes d'une attaque par rançongiciel à répétition.

Si vous croyez être la victime d'une attaque par rançongiciel :

1. Lisez les conseils sur la façon de se remettre d'une cyberattaque à la section Se défendre contre les cybermenaces.
2. Signalez l'incident lié à un rançongiciel :
    a. au service de police local;
    b. au Centre antifraude du Canada;
    c. au Centre pour la cybersécurité.
3. Après avoir entrepris les efforts de reprise, consultez la section Se remettre d'un incident lié à un rançongiciel pour savoir comment améliorer votre environnement de cybersécurité.

Table des matières

Liste des figures

Découvrir les rançongiciels

Un rançongiciel est un type de maliciel qui bloque l'accès aux fichiers ou aux systèmes jusqu'à ce que l'utilisateur verse une somme d'argent. Les rançongiciels ont évolué et englobent des incidents se traduisant plutôt par le vol de données et l'extorsion. Les incidents liés à des rançongiciels peuvent détruire votre organisation en perturbant vos processus opérationnels et fonctions essentielles qui dépendent de la connectivité des réseaux et des systèmes. Pour en savoir plus sur l'évolution des menaces de rançongiciel au Canada, consultez la publication intitulée « Vue d'ensemble des menaces par rançongiciel de 2025 à 2027 ».

Fonctionnement d'un rançongiciel

Lorsqu'un rançongiciel infecte un dispositif, il verrouille le système ou chiffre la fonction de stockage, empêchant ainsi l'accès à l'information et aux systèmes sur vos dispositifs. Les auteurs de menace peuvent aussi utiliser votre réseau compromis pour propager le rançongiciel dans d'autres systèmes et dispositifs connectés.

Vos réseaux et dispositifs peuvent être infectés par un rançongiciel à la suite de l'une ou l'autre des activités suivantes :

- consulter des sites Web non sécurisés, suspects ou compromis;
- ouvrir des pièces jointes ou des fichiers infectés provenant de sources connues ou inconnues;
- cliquer sur des liens dans des courriels, des médias sociaux et des réseaux pair à pair;
- insérer un périphérique infecté (par exemple, une clé USB) dans un différent dispositif;
- exposer ses systèmes à Internet inutilement ou sans avoir mis en place des mesures robustes en matière de sécurité et de maintenance, par exemple,
    - ne pas mettre en place des systèmes de détection et de prévention des intrusions (SDPI),
    - piloter des dispositifs en fin de vie ou non corrigés,
    - ne pas utiliser l'authentification multifacteur (AMF).

Si votre organisation est victime d'une attaque par rançongiciel, les utilisatrices et utilisateurs de même que les administratrices et administrateurs recevront un avis leur indiquant que des fichiers ont été chiffrés et qu'ils seront inaccessibles jusqu'à ce qu'une rançon soit payée. Vous pourriez également recevoir sur votre écran verrouillé un message indiquant que votre dispositif est verrouillé

et inaccessible jusqu'à ce que vous payiez une rançon. Le message vous ordonnera de payer la rançon pour pouvoir déverrouiller le dispositif et récupérer les fichiers.

Les cybercriminelles et cybercriminels demandent habituellement la rançon en cryptomonnaie, parce qu'il peut être difficile d'établir l'origine du transfert. Le Centre d'analyse des opérations et déclarations financières du Canada a affirmé en 2023 que le mouvement des recettes découlant de la fraude et des attaques par rançongiciel constitue la méthode de blanchiment d'argent la plus répandue liée aux monnaies virtuelles. On pourrait aussi vous demander de payer avec des cartes de crédit prépayées ou des cartes-cadeaux. Les auteurs de menace vous accorderont un délai fixé pour payer la rançon, après quoi ils pourraient augmenter le montant de la rançon, détruire vos fichiers de façon permanente ou divulguer vos données. Les tactiques plus sophistiquées peuvent comprendre la double extorsion. Un auteur de menace vole les données d'une victime, avant de les chiffrer. C'est donc dire que la victime fait face à deux menaces : elle doit payer une rançon pour faire déchiffrer ses données, puis payer une autre rançon pour empêcher que ses données volées soient divulguées au public.

Selon l'Évaluation des cybermenaces nationales 2025-2026 (ECMN), les auteurs de menace améliorent sans cesse leurs stratégies et adaptent leurs techniques afin de maximiser leurs profits et d'éviter la détection par les forces policières. Les motivations financières et la souplesse du modèle de rançongiciel-service (RaaS pour *Ransomware-as-a-Service*) ont presque assurément renforcé la résistance des auteurs de menace face aux mesures de perturbation prises par les forces policières.

Les attaques par rançongiciel sont devenues plus sophistiquées et leurs auteurs emploient souvent une combinaison de vecteurs d'attaque. Il peut s'agir de l'envoi à votre organisation d'un courriel d'hameçonnage ou de la conduite d'attaques sur les mécanismes d'authentification, au cours desquelles ils y vont de nombreuses tentatives de connexion ou de supposition de mot de passe pour accéder à vos systèmes.

Un rançongiciel peut également se propager dans les systèmes et réseaux d'autres organisations connectées par l'entremise de chaînes d'approvisionnement. Par exemple, une organisation qui fournit des services à la clientèle au moyen de réseaux interconnectés et de systèmes de gestion client pourrait être ciblée par un rançongiciel. L'auteur de menace pourrait alors se servir des réseaux interconnectés ou des systèmes de gestion client pour infecter au moyen d'un rançongiciel d'autres organisations au sein de la chaîne d'approvisionnement. Ces organisations n'auraient donc plus accès à leurs systèmes, et leurs opérations seraient perturbées.

La nouvelle génération d'intelligence artificielle (IA), l'IA agentive, pose un risque important pour la cybersécurité en permettant des opérations de rançongiciel qui sont :

- **autonomes** : les agents d'IA ne dépendent plus de l'intervention humaine et peuvent agir indépendamment tout au long du cycle de vie des attaques;
- **efficaces** : des activités comme la reconnaissance, l'exploitation et le chiffrement, qui prenaient autrefois des jours ou des semaines, peuvent maintenant être comprimées en minutes;
- **adaptatives** : les agents peuvent évaluer leur environnement, sélectionner des tactiques optimales, échapper à la détection et se remettre de tentatives ratées de façon dynamique;
- **secrètes** : l'IA qui permet d'effacer des traces et de brouiller les pistes rend les enquêtes judiciaires beaucoup plus difficiles.

En pratique, l'IA agentive peut découvrir des points faibles dans un réseau, contourner les mécanismes de défense, déployer des maliciels et supprimer les preuves de l'intrusion, le tout dans un seul flux d'activités géré par l'IA. Toutefois, tout comme l'IA agentive pose un nouveau défi en matière de cybersécurité, elle offre également des avantages défensifs potentiels. Les équipes de sécurité pourraient déployer des agents d'IA autonomes pour surveiller les réseaux, détecter les anomalies ou même créer des systèmes leurres qui trompent les auteurs. Ces agents peuvent détecter les premiers signes d'intrusion, comme le chiffrement soudain des fichiers, les tentatives d'accès non autorisées ou les mouvements latéraux anormaux dans les systèmes. Contrairement aux outils de surveillance traditionnels, l'IA agentive ne repose pas uniquement sur les signatures connues; elle recourt à l'analyse comportementale et à la détection des anomalies pour repérer les menaces nouvelles ou furtives qui pourraient autrement passer inaperçues.

Lorsqu'une menace de rançongiciel est détectée, l'IA agentive peut déclencher de façon autonome une intervention rapide en cas d'incident. Il peut s'agir d'isoler les points terminaux infectés du réseau, de mettre fin aux processus malveillants, de restaurer des fichiers à partir de sauvegardes sécurisées et d'aviser les équipes de sécurité. Ces actions, qui prennent habituellement des minutes ou des heures lorsqu'elles sont effectuées manuellement, peuvent être exécutées en quelques secondes, ce qui réduit considérablement l'incidence d'une attaque.

Il est essentiel d'évaluer soigneusement les risques et d'établir une surveillance appropriée lors de l'intégration de l'IA dans une chaîne de détection et d'atténuation des rançongiciels. Tenir compte des mesures de protection suivantes :

- Catégorisation des données : Catégoriser les données à chaque étape (formation, validation, inférence et surveillance) afin d'évaluer les facteurs de risque liés à la protection des renseignements personnels, à la sécurité, à la robustesse et aux considérations morales.

- Plus qu'une assurance logicielle standard : Évaluer la qualité des données d'entrée, les cas d'usage du modèle et les dépendances du système. Mettre en correspondance les procédures de vérification de l'IA et les contrôles de sécurité du guide La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) du Centre pour la cybersécurité, adaptés au profil de risque de l'organisation.
- Surveillance continue : Utiliser des outils automatisés pour la détection des anomalies, la dérive des extrants et la télémétrie du système. Surveiller de près les mises à jour non autorisées du modèle ou les changements imprévus de comportement. Il est impératif d'établir de solides mécanismes d'audit, de journalisation et d'intervention en cas d'incident aux fins de responsabilisation et d'analyse criminalistique.
- Mesures de protection et contrôles : Mettre en place des mesures de protection techniques pour les entrées et sorties de données et pour les interfaces API (API pour Application Programming Interface) et, le cas échéant, appliquer les normes du protocole MCP (*Model-Context-Protocol*). Les mesures de protection doivent tenir compte des fonctionnalités multilingues du modèle et empêcher toute mauvaise utilisation dans les langues humaines et informatiques.
- Surveillance avec intervention humaine : Veiller à ce que les décisions critiques en matière d'intervention soient prises par du personnel qualifié afin de réduire au minimum les risques associés aux faux positifs et négatifs, aux hallucinations ou à la manipulation antagoniste des grands modèles de langage. Éviter la prise de décisions automatisée à grande incidence sans intervention humaine.
- Réentraînement périodique : Dans le cas des modèles gérés localement, procéder à un réentraînement de routine à partir de jeux de données validés, diversifiés et non biaisés afin de maintenir la résilience et de réduire les risques systémiques.
- Gouvernance et responsabilisation : Élaborer et tenir à jour des politiques organisationnelles, des structures de responsabilité et des rôles axés sur la surveillance de la gestion des risques tout au long du cycle de vie de l'IA, conformément au cadre de gestion des risques liés à l'IA [en anglais seulement] du National Institute of Standards and Technology et aux directives du Centre pour la cybersécurité. Advenant son déploiement au gouvernement du Canada, s'assurer que la Directive sur la prise de décisions automatisée du Secrétariat du Conseil du Trésor du Canada est respectée.

L'IA agentive représente un changement majeur dans le contexte de la cybersécurité, offrant à la fois de meilleures capacités offensives aux auteurs et de nouveaux moyens de défense puissants aux organisations.

La figure 1 ci-après illustre les manières dont un rançongiciel peut affecter les réseaux et les dispositifs d'une organisation. On y retrouve les trois principaux vecteurs d'accès fréquemment utilisés dans les incidents liés aux rançongiciels :

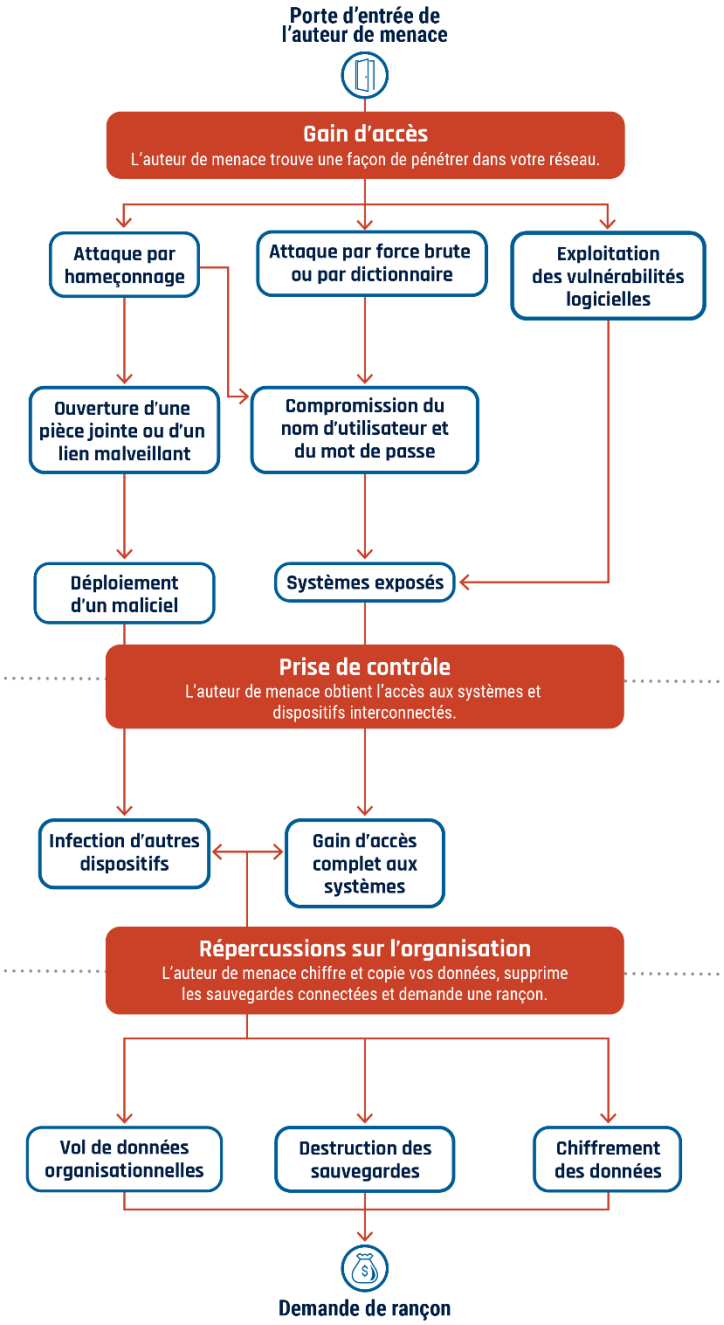
- les attaques sur les mécanismes d'authentification (supposition de mot de passe);
- l'exploitation de vulnérabilités dans les logiciels;
- la conduite d'attaques par hameçonnage.

La figure 1 démontre également les trois étapes d'un incident lié à un rançongiciel :

1. L'auteur de menace obtient l'accès à votre réseau.
2. Il prend le contrôle de vos systèmes et dispositifs connectés.
3. Il déploie la charge du maliciel pour infecter vos systèmes et dispositifs connectés au moyen d'un rançongiciel.

Lorsque l'auteur de menace obtient le plein contrôle de votre réseau, de vos systèmes et de vos dispositifs, il peut chiffrer vos données, supprimer les fichiers de sauvegarde connectés et voler les données de votre organisation. L'auteur peut menacer de divulguer ces données si vous refusez de payer la rançon, ou il peut vous laisser croire qu'il déchiffrera vos données et rétablira votre accès si vous payez la rançon.

Figure 1: Déroulement des incidents liés aux rançongiciels



Description longue – Figure 1 : Déroulement des incidents liés aux rançongiciels

Cette image illustre la méthodologie qu'utilise habituellement un auteur de menace pour accéder à votre réseau, à vos systèmes et à vos dispositifs connectés. Un incident lié à un rançongiciel se produit en trois étapes. L'auteur de menace :

- trouve une façon de pénétrer dans votre réseau, vos systèmes ou vos dispositifs;
- prend le contrôle et déploie le rançongiciel;
- chiffre vos données, détruit vos sauvegardes et vole les données de l'organisation pour ensuite demander le paiement d'une rançon afin de rétablir votre accès.

Au cours de la première étape de l'incident lié au rançongiciel, l'auteur de menace trouve habituellement une façon de pénétrer dans votre réseau par les moyens suivants :

- Force brute (supposition de mot de passe)
- Vulnérabilités dans les logiciels
- Attaques par hameçonnage
    - L'auteur de menace tente de solliciter de l'information confidentielle appartenant à un individu, à un groupe ou à une organisation en les usurpant ou en imitant une marque commerciale connue, souvent dans le but de réaliser des gains financiers.
    - Les hameçonneuses et hameçonneurs incitent les utilisatrices et utilisateurs à divulguer des renseignements personnels (numéros de carte de crédit, identifiants de connexion bancaire en ligne ou autres renseignements sensibles) afin de s'en servir pour commettre des actes frauduleux.

Après avoir obtenu l'accès à votre réseau, l'auteur de menace passe à la deuxième étape, qui consiste à prendre le contrôle de vos systèmes et de vos dispositifs connectés. Il déploie ensuite la charge du maliciel et infecte vos systèmes et dispositifs connectés au moyen d'un rançongiciel.

Lorsque l'auteur obtient le plein contrôle, il passe à la troisième étape, qui consiste à chiffrer vos données, à supprimer les fichiers de sauvegarde disponibles ou connectés et, souvent, à voler les données de votre organisation. L'auteur peut menacer de divulguer ces données si vous refusez de payer la rançon, ou il peut vous laisser croire qu'il déchiffrera vos données et rétablira votre accès si vous payez la rançon.

Vecteurs de rançongiciel communs

Les auteurs de menace peuvent exploiter de nombreuses vulnérabilités et de nombreux vecteurs d'attaque pour infecter au moyen d'un rançongiciel votre réseau, vos systèmes et vos dispositifs. Voici des exemples des vecteurs de rançongiciel les plus souvent utilisés par les auteurs de menace.

Cybercriminalité comme service

Les auteurs de menace spécialisés recourent à la cybercriminalité comme service (CaaS pour *Cybercrime-as-a-Service*) pour vendre en ligne à d'autres cybercriminelles et cybercriminels des données volées ou fuitées et des outils malveillants prêts à l'emploi, leur permettant ainsi d'exercer leurs activités illégales. L'écosystème de la CaaS est soutenu par des marchés en ligne en pleine expansion.

Rançongiciel-service

Un RaaS est un modèle opérationnel de CaaS selon lequel un auteur de menace, peu importe ses compétences, peut acheter un maliciel d'un développeur sur le Web clandestin. Le développeur reçoit ensuite une partie de la rançon versée par la victime. La plupart des principaux groupes d'exploitation de rançongiciels qui sévissent au Canada recourent au modèle opérationnel de RaaS selon lequel un noyau d'opératrices et opérateurs vend ou loue sa variante de rançongiciel à des affiliés qui lancent les attaques. Dans l'ECMN 2025-2026, on estime que la popularité soutenue du RaaS contribue presque certainement à l'augmentation du nombre d'incidents liés à des rançongiciels, étant donné qu'il réduit les obstacles techniques et administratifs à l'entrée et permet à un plus grand nombre d'auteurs de lancer des attaques.

Hameçonnage

L'hameçonnage est un type d'attaque par piratage psychologique dans le cadre duquel on utilise un texte, un courriel ou les médias sociaux pour inciter les utilisatrices et utilisateurs à cliquer sur un lien malveillant ou une pièce jointe malveillante, à révéler de l'information sensible ou à apporter un changement dans un système. Les tentatives d'hameçonnage prennent souvent la forme d'un envoi massif de messages généraux qui peuvent sembler légitimes et provenir d'une source de confiance, comme une institution financière. Pour en savoir plus sur l'hameçonnage, consultez la publication Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101).

Téléchargement furtif

Le téléchargement furtif se produit lorsqu'une utilisatrice ou un utilisateur visite, sans le savoir, un site Web infecté qui entraîne le téléchargement, puis l'installation d'un maliciel, toujours à son insu.

Placement de publicité malveillante

Le placement de publicité malveillante permet d'injecter un code malveillant dans des publicités légitimes en ligne. Lorsqu'une utilisatrice ou un utilisateur clique sur la publicité, un maliciel se propage dans son dispositif. Certaines publicités malveillantes n'exigent même pas l'intervention des utilisatrices et utilisateurs et peuvent distribuer du code malveillant simplement en étant affichées.

Services exposés

Les services exposés, comme le protocole RDP (pour *Remote Desktop Protocol*) et les systèmes de gestion de contenu, donnent accès à vos systèmes. Les auteurs de menace ont recours à diverses tactiques, comme l'exploitation des vulnérabilités courantes et la rafale de mots de passe, pour accéder à vos dispositifs par les systèmes exposés et déployer un rançongiciel.

Usurpation d'adresse électronique

Les auteurs de menace peuvent utiliser les identités de fournisseurs de services gérés (FSG) et les identités d'autres tiers pour usurper des adresses électroniques ou mener des attaques par hameçonnage contre votre organisation. Pour en savoir plus sur la façon de mieux protéger votre organisation contre ces types de menace, consultez la publication Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030).

Attaque de la chaîne d'approvisionnement

L'attaque de la chaîne d'approvisionnement permet aux auteurs de menace d'infiltrer un organisme fournisseur de services et de forcer les utilisatrices et utilisateurs connectés à effectuer une mise à jour, ce qui peut ensuite infecter leurs systèmes et dispositifs au moyen d'un rançongiciel. Le Centre pour la cybersécurité fournit des conseils sur la façon de sécuriser la chaîne d'approvisionnement de votre organisation dans la publication Cybersécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations (ITSAP.00.070).

Entités ciblées par des rançongiciels

Dans l'ECMN 2025-2026, le Centre pour la cybersécurité a déterminé que les activités de rançongiciel dirigées contre le Canada continueront probablement à cibler les grandes entreprises ainsi que les grands fournisseurs d'infrastructures essentielles. Cependant, cette observation ne signifie pas que d'autres organisations ou personnes sont nécessairement à l'abri des rançongiciels. N'importe quelle organisation peut en être victime si elle compte sur des données pour mener à bien ses activités. Selon l'ECMN, au cours des deux prochaines années, les opératrices et opérateurs de rançongiciels intensifieront presque certainement leurs tactiques d'extorsion et perfectionneront leur capacité d'accroître la pression exercée sur les victimes pour qu'elles paient des rançons et d'échapper aux forces policières.

Comme pour la majorité des cybercriminelles et cybercriminels, les auteurs d'attaques par rançongiciel sont motivés par l'appât du gain. Ils ciblent des organisations de toutes tailles et exigent un montant en rançon basé sur ce qu'ils croient que l'organisation sera prête à payer pour récupérer ses données chiffrées.

Les attaques par rançongiciel peuvent avoir de graves répercussions, notamment :

- des atteintes à la protection des données et à la vie privée;
- des atteintes à la réputation;
- une perte de productivité;
- des conséquences juridiques;
- des coûts de reprise;
- des dommages à l'infrastructure et aux opérations.

Les opératrices et opérateurs de rançongiciels profitent presque certainement des occasions qui se présentent à eux et ne visent aucune industrie en particulier. Toutefois, les rançongiciels sont la principale menace de la cybercriminalité qui plane sur les infrastructures essentielles du Canada, car ils peuvent paralyser des opérations essentielles, détruire ou endommager des données commerciales importantes et révéler de l'information sensible. En plus d'engendrer des pertes financières découlant de la réparation et restauration des systèmes et de la reprise des opérations, les attaques par rançongiciel peuvent ébranler les services essentiels et ainsi mettre en péril la sécurité et le bien-être des victimes et des personnes tributaires des services.

Les infrastructures essentielles sont une cible attrayante pour les opératrices et opérateurs de rançongiciels, qui les considèrent comme étant disposées à payer d'importantes rançons pour

protéger leurs opérations essentielles. Selon l'ECMN, les victimes d'attaques par rançongiciel en 2023 étaient moins enclines à payer les rançons demandées. La perspective d'engranger d'importants profits, jumelée à la volonté décroissante des victimes de verser des rançons, ont presque certainement encourager les groupes d'exploitation de rançongiciels plus avancés sur le plan technique à rehausser leurs techniques d'extorsion et à embaucher des affiliés compétents capables de cibler des entités des infrastructures essentielles pour empocher des rançons plus importantes.

Les petites et moyennes organisations sont également des cibles puisque les auteurs de menace jugent que leurs mesures de sécurité sont faibles et qu'elles sont donc prédisposées aux attaques. Il est fort probable que les petites et moyennes organisations canadiennes qui sont victimes d'attaques par rançongiciel continueront d'acquiescer aux demandes de rançon au lieu de perdre des marchés ou d'avoir à reconstruire leurs réseaux. Il est également probable qu'elles craignent de subir les conséquences potentiellement dévastatrices du refus de payer.

Les auteurs de cybermenace volent souvent de l'information lors d'une attaque par rançongiciel. Ils gardent les données en attendant le paiement de la rançon, les vendent ou les utilisent pour obtenir un avantage concurrentiel inéquitable en exploitant des renseignements exclusifs ou brevetés. Le vol de renseignements organisationnels, dont la propriété intellectuelle et les données de la clientèle, peut avoir des répercussions financières à court et à long terme pour les victimes. Il s'agit notamment de répercussions sur la compétitivité à l'échelle internationale, d'atteintes à la réputation et de vol d'identité.

La concentration des fournisseurs augmente la vulnérabilité des organisations aux cybermenaces, comme les rançongiciels. Quelques grands fournisseurs de services numériques, chacun d'entre eux comptant un grand parc d'utilisatrices et utilisateurs, fournissent de nombreux services technologiques. Un cyberincident mettant en cause un seul fournisseur de services dominant peut donc toucher l'ensemble d'un secteur. Les fournisseurs dominants sont ciblés par les auteurs de cybermenace qui cherchent à voler les données de la clientèle ou à réclamer des rançons. La compromission de fournisseurs de services dominants peut amplifier l'impact des incidents de cybersécurité. Les activités de cybermenace contre des services qui représentent de véritables goulots d'étranglement numériques (points de défaillance uniques dans les chaînes d'approvisionnement) peuvent engendrer des perturbations en chaîne et généralisées pour l'économie et la société, et mettre en péril la sécurité nationale.

Enfin, l'exposition aux cybermenaces augmente. Outre l'adoption et le déploiement continus de l'Internet des objets (par exemple, les véhicules connectés), il est prévu que l'essor des services et

des plateformes d'IA stimulera la demande pour les infrastructures de soutien et mènera au transfert de volumes encore plus élevés de données aux environnements infonuagiques. Il est aussi très probable que les organisations spécialisées dans l'IA soient maintenant des cibles plus importantes pour les auteurs de cybermenace et les rançongiciels.

Versement d'une rançon

Il est difficile de prendre la décision de payer une ou un cybercriminel pour qu'il vous redonne l'accès à vos fichiers, et vous ressentirez probablement l'obligation d'acquiescer à ses demandes. Avant même d'envisager de payer, communiquez avec le service de police local pour signaler le cybercrime. Payer la rançon demandée ne garantira pas pour autant l'accès à vos données chiffrées ou à vos systèmes.

C'est à votre organisation que revient la décision de payer ou non la rançon. Cela dit, il est important de bien comprendre les risques associés à la décision de payer. Par exemple, il est possible que les auteurs de menace utilisent un effaceur. Il s'agit d'un maliciel qui altère ou supprime de façon permanente vos fichiers une fois la rançon payée. Le paiement de la rançon valide également le RaaS comme modèle opérationnel, ce qui favorisera sa croissance et financera de nouvelles attaques. La somme versée pourrait également servir à financer d'autres activités illégales, comme le crime organisé, le terrorisme ou la violence parrainée par l'État. De plus, il peut être illégal de payer une rançon en vertu des lois contre le terrorisme, le blanchiment d'argent et le financement d'activités d'organisations criminelles ou des lois autorisant l'imposition de sanctions. Même si vous payez la rançon, les auteurs de menace pourraient quand même :

- demander plus d'argent;
- continuer d'infecter vos dispositifs et systèmes ou ceux d'autres organisations;
- attaquer votre organisation à nouveau;
- copier, divulguer ou vendre vos données.

L'ECMN 2025-2026 illustre le nombre relatif d'incidents liés à des rançongiciels au Canada signalés au Centre pour la cybersécurité par des victimes canadiennes entre 2021 et 2024. D'après nos données, le nombre d'incidents liés à des rançongiciels a augmenté, en moyenne, de 26 % d'année en année. Étant donné que de nombreux incidents liés à des rançongiciels ne sont pas signalés, il est presque certain que le nombre réel de ces incidents visant le Canada est plus élevé que ce qui est indiqué. L'Enquête canadienne sur la cybersécurité et le cybercrime (ECCC), menée par Statistique Canada pour le compte de Sécurité publique Canada, a fait remarquer que les coûts de reprise totaux

associés aux incidents de cybersécurité en 2023 ont doublé pour s'établir à 1,2 milliard de dollars canadiens.

Se défendre contre les cybermenaces

Les rançongiciels figurent parmi les types de maliciel les plus répandus et constituent potentiellement l'une des cyberattaques les plus dommageables pour votre organisation. Les mesures isolées d'atténuation ne sont pas suffisamment rigoureuses pour lutter contre la menace en constante évolution des rançongiciels. Votre organisation doit adopter une stratégie de défense en profondeur (à plusieurs niveaux) pour protéger ses dispositifs, systèmes et réseaux contre les rançongiciels et contre d'autres types de maliciel et de cyberattaque. Votre stratégie doit comprendre de multiples niveaux de défense, ainsi que plusieurs mesures d'atténuation ou contrôles de sécurité à chaque niveau.

Planification de la cyberdéfense

Il existe de nombreuses approches que vous pouvez adopter pour mieux protéger vos réseaux, vos systèmes et vos dispositifs. Vous trouverez ci-dessous une liste des contrôles de sécurité que vous pouvez mettre en œuvre pour renforcer votre posture de cybersécurité.

Élaborer un plan de sauvegarde

Élaborez et mettez en œuvre un plan de sauvegarde pour votre organisation. Une copie de sauvegarde vous permettra de récupérer vos données et systèmes dans l'éventualité d'un incident. Il existe plusieurs types de sauvegarde que vous pouvez mettre en œuvre pour protéger les données de votre organisation :

- **Sauvegarde complète :** Il vaut mieux faire une sauvegarde complète de façon périodique (chaque semaine ou chaque mois) et avant chaque mise à niveau majeure du système. C'est l'option la plus coûteuse en argent et en temps, selon le volume de données à sauvegarder et vos besoins en matière de stockage.
- **Sauvegarde différentielle :** Ce type de sauvegarde consiste à faire seulement une copie des données qui ont changé depuis la dernière sauvegarde complète.
- **Sauvegarde incrémentielle :** Ce type de sauvegarde consiste à stocker uniquement les données qui ont changé depuis la dernière sauvegarde complète ou différentielle. Chaque incrément est sauvegardé en tant que volume incrémentiel. Si vous devez restaurer des données, vous devez traiter chaque incrément, ce qui peut prendre du temps.

Stocker des sauvegardes

Il y a trois options de stockage pour vos sauvegardes : en ligne, hors ligne et dans le nuage.

Les sauvegardes en ligne :

- sont stockées dans l'espace physique de votre organisation;
- sont faciles d'accès si vous devez lancer votre processus de reprise;
- sont susceptibles à une perte de données en cas de catastrophe naturelle ou de panne d'électricité;
- sont vulnérables aux rançongiciels si elles sont connectées à vos systèmes ou à vos réseaux.

Les sauvegardes hors ligne (ou « sauvegardes à froid ») :

- sont stockées à des emplacements physiques distincts, à l'extérieur des installations principales de votre organisation;
- ne sont pas connectées à vos réseaux.

Bien que le vol ou la perte de données demeure une possibilité, le stockage hors ligne peut empêcher les auteurs de menace d'accéder à vos sauvegardes et de les infecter à l'aide d'un rançongiciel.

Les sauvegardes dans le nuage :

- sont stockées sur une plateforme infonuagique, qui est souvent gérée par un fournisseur de services infonuagiques (FSI);
- sont accessibles au moyen du serveur de votre FSI, à partir de n'importe quel endroit;
- sont chiffrées dans le nuage par mesure de sécurité supplémentaire, mais la perte de données et les cyberattaques (y compris les rançongiciels) peuvent quand même se produire.

Protéger ses sauvegardes

Beaucoup de variantes de rançongiciel ont été conçues de façon à repérer et à supprimer les sauvegardes de vos systèmes et à s'y propager. Par ces actions, les auteurs de menace augmentent la probabilité que votre organisation paie la rançon demandée. Si le rançongiciel se propage dans vos sauvegardes, vous ne serez pas en mesure de récupérer vos systèmes et vos données et, en fin de compte, cette situation entraînera l'arrêt de vos activités. Les sauvegardes les plus courantes, soit celles stockées en ligne ou dans le nuage, sont exposées aux rançongiciels. Le recours au stockage des sauvegardes de votre organisation hors ligne est la méthode qui offre la plus grande protection contre les incidents liés aux rançongiciels.

Votre organisation doit pouvoir mettre en œuvre un processus de sauvegarde hors ligne. Ainsi, vos sauvegardes ne seront pas connectées à vos réseaux ou dispositifs, ce qui signifie que le rançongiciel ne peut pas repérer et supprimer vos sauvegardes. Votre organisation doit veiller à stocker plusieurs copies des sauvegardes hors ligne. Le processus de sauvegarde doit être effectué fréquemment afin de garantir que les données sont, dans la mesure du possible, en temps réel. Tester les sauvegardes est aussi un élément essentiel du processus de sauvegarde et de reprise. Il est recommandé de chiffrer les sauvegardes pour ainsi profiter d'une couche supplémentaire de protection. Les Conseils sur la mise en œuvre de l'agilité cryptographique (ITSAP.40.018) et la Boîte à outils des objectifs relatifs à l'état de préparation en matière de cybersécurité intersectoriels du Centre pour la cybersécurité offrent des renseignements sur le chiffrement fort et agile des données en transit.

Il est aussi recommandé d'avoir une deuxième sauvegarde dans le nuage pour améliorer votre capacité de reprise. Ces sauvegardes seront idéalement gérées par un FSI à même son infrastructure infonuagique sécurisée. Les FSI offrent à votre organisation une couche de sécurité supplémentaire. Veuillez noter que votre organisation est en tout temps légalement responsable de la protection de ses données. Vous devez vous assurer que le fournisseur de services que vous sélectionnez peut prendre en charge vos exigences de sécurité, de sauvegarde et de reprise au moyen de mécanismes de protection appropriés. Vous devriez également envisager la résidence des données, ce qui fait référence à l'emplacement géographique où vos données sont stockées. Il est possible que votre organisation ait des exigences réglementaires et politiques qui exigent que les données soient stockées au Canada. Si vous envisagez de faire appel à un fournisseur pour le stockage hors site, assurez-vous qu'il dispose de mesures de sécurité, de processus de gestion des incidents et d'un plan de reprise après sinistre.

Remarque : Votre FSI peut aussi être victime d'un rançongiciel, ce qui pourrait avoir indirectement des répercussions sur votre organisation. Ne pas avoir accès aux données qui sont stockées dans le nuage peut avoir une incidence considérable sur la gestion de vos activités. Vous pourriez également être aux prises avec des problèmes d'intégrité et de confidentialité des données.

Recommandation : L'approche recommandée pour sauvegarder votre information est d'avoir plusieurs sauvegardes à plusieurs endroits. Vous devriez avoir au moins deux sauvegardes stockées hors ligne auxquelles il est impossible d'accéder au moyen d'une connexion réseau ou Internet. Vous pourriez ensuite avoir une sauvegarde secondaire dans le nuage gérée par votre FSI. Par ailleurs, vous devriez établir un calendrier pour tester régulièrement vos processus de sauvegarde (par exemple, tous les mois). En ayant au moins une copie de sauvegarde de vos fichiers, votre

organisation a davantage de chances de se remettre d'une attaque par rançongiciel, ou de tout autre cyberincident, et de reprendre plus rapidement ses activités.

Pour obtenir de plus amples renseignements sur l'élaboration d'un plan de sauvegarde, consultez la publication Sauvegarder et récupérer vos données (ITSAP.40.002).

Élaborer un plan d'intervention en cas de cyberincident

Élaborer un plan d'intervention en cas d'incident pour votre organisation est la clé de votre stratégie de cyberdéfense. Vous devriez également envisager d'élaborer un plan de reprise après sinistre pour votre organisation. Dans ces deux plans, votre organisation tient compte des événements majeurs qui pourraient provoquer une panne imprévue et l'obliger à activer son plan d'intervention. Le plan d'intervention en cas d'incident vous aide à détecter des incidents de cybersécurité et à intervenir. Le plan de reprise après sinistre est axé sur les moyens que doit prendre votre organisation pour se remettre d'un incident et reprendre ses activités essentielles.

Il existe de nombreux avantages à l'élaboration d'un plan d'intervention en cas d'incident :

- une gestion efficace des incidents minimise les répercussions d'un cyberincident;
- un plan qui aura été mis en pratique au préalable vous aidera à prendre de bonnes décisions sous la pression de gérer un réel incident;
- comme les mesures principales sont approuvées à l'avance, vous disposez immédiatement des ressources et pouvoirs financiers requis pour intervenir en cas d'incident;
- une intervention bien gérée, accompagnée d'une communication claire tout au long du processus, met en confiance les parties prenantes et la clientèle;
- les leçons tirées des incidents permettent de repérer les lacunes et les problèmes en ce qui a trait à votre capacité d'intervention.

Votre plan d'intervention en cas d'incident doit comprendre plusieurs éléments clés. L'objectif principal est de se remettre d'un incident le plus rapidement possible. La liste de vérification suivante donne un aperçu des éléments clés à inclure dans votre plan d'intervention en cas d'incident. Il ne s'agit pas d'une liste complète d'exigences en matière d'intervention en cas d'incident, mais elle fournit une approche structurée ainsi que des mesures que votre organisation peut mettre en œuvre.

En suivant cette liste lors des étapes préliminaires de votre plan d'intervention, vous pouvez déterminer vos risques, concevoir un plan d'action pour les atténuer, et préparer votre organisation à une reprise efficace qui lui permettra de se remettre en marche rapidement.

Pour obtenir de plus amples renseignements sur l'élaboration d'un plan d'intervention en cas d'incident, consultez la publication Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003).

Liste de vérification du plan d'intervention en cas de cyberincident

Recourez à la liste de vérification suivante du plan d'intervention en cas d'incident pour vous assurer que votre intervention est complète.

- Mener une évaluation des risques :
  - Déterminez les principaux systèmes et biens qui sont essentiels à vos opérations.
  - Analysez la probabilité et les répercussions d'une compromission de ces systèmes.
  - Orientez les efforts d'intervention de façon à protéger les systèmes et les biens les plus importants et à en effectuer la sauvegarde hors ligne fréquemment et en toute sécurité.
- Élaborer des politiques et procédures :
  - Élaborez une politique d'intervention en cas d'incident qui établit les pouvoirs, les rôles et les responsabilités de votre organisation.
  - Mettez en place les autorisations préalables d'impartir un contrat d'assistance et communiquez les détails connexes aux responsables clés de l'intervention en cas d'incident.
- Établir une équipe d'intervention en cas de cyberincident :
  - Créez une équipe d'intervention en cas de cyberincident pour
    - évaluer les incidents, les documenter et y intervenir;
    - rétablir vos systèmes et récupérer l'information;
    - réduire le risque qu'un autre incident lié à un rançongiciel se produise.
  - Cette équipe doit être composée d'employées et employés qui ont diverses compétences. Elle devra également pouvoir compter sur un soutien interfonctionnel de la part d'autres secteurs d'activités.
  - Nommez des intervenantes et intervenants qui peuvent venir en renfort en l'absence de membres de l'équipe d'intervention dans l'éventualité d'un incident.
- Offrir de la formation :
  - Adaptez vos programmes de formation aux exigences et aux besoins opérationnels de votre organisation, ainsi qu'aux rôles et aux responsabilités des employées et employés.

- Assurez-vous que la formation fait état des contrôles de cybersécurité énumérés à la section Contrôles de cybersécurité (par exemple, comment repérer les courriels malveillants et les attaques par hameçonnage et utiliser des phrases de passe robustes).
- Pour obtenir des avis et conseils sur la formation en matière de gestion des événements de cybersécurité, envoyez un courriel au Carrefour de l'apprentissage du Centre pour la cybersécurité à l'adresse education@cyber.gc.ca. Le Carrefour de l'apprentissage offre un cours complet sur la gestion des événements pouvant être adapté aux besoins opérationnels et en matière de technologie de l'information (TI) de votre organisation.

- Désigner les parties prenantes :
  - Dressez la liste des principales parties prenantes internes et externes qui seront informées d'un incident. Vous pourriez avoir à informer des tiers, comme des clients ou des FSG.
  - Selon la nature de l'incident, vous pourriez avoir à communiquer avec la police et, si nécessaire, avec un bureau de consultation juridique.
- Dresser un plan de communication:
  - Décrivez en détail comment, quand et avec qui votre équipe communique.
  - Déterminez un point de contact central à qui les employées et employés doivent signaler les incidents soupçonnés ou connus.
  - Assurez-vous d'avoir les coordonnées externes des membres titulaires et des remplaçantes et remplaçants de votre équipe d'intervention, des membres du personnel essentiel et des principales parties prenantes.
  - Préparez des modèles de déclaration aux médias pouvant être adaptés aux cyberincidents au moment où ils se produisent.
  - Évaluez la possibilité de retenir les services d'une organisation tierce de reprise après sinistre (rançongiciel) qui peut vous accompagner tout au long de votre intervention et de votre processus de reprise.

Processus d'intervention en cas d'incident

Votre processus d'intervention en cas d'incident suivra un cycle en quatre étapes.

Étape 1 : Préparation

- Élaborez les politiques.
- Définissez les objectifs.
- Mettez à l'essai les processus de sauvegarde.
- Mettez à l'essai les processus d'application des correctifs et des mises à jour.
- Trouvez les vulnérabilités.
- Concevez des exercices de mise à l'essai.

Étape 2 : Observation

- Élaborez une stratégie de surveillance (par exemple, fréquence, réseaux inclus).
- Surveillez vos réseaux et vos dispositifs connectés pour repérer les menaces.
- Produisez régulièrement des rapports d'événement et d'incident.
- Analysez les données et déterminez si vous devez activer le plan d'intervention.

Étape 3 : Résolution

- Analysez les constatations afin de bien comprendre l'incident.
- Déterminez les mesures d'atténuation que vous devez mettre en place (par exemple, déconnecter les dispositifs).
- Exécutez un antimaliciel et un antivirus.
- Corrigez les vulnérabilités.
- Récupérez vos données et systèmes à l'aide de votre copie de sauvegarde.
- Conservez les preuves et documentez les étapes que vous avez mises en œuvre.

Étape 4 : Compréhension

- Déterminez la cause fondamentale de l'incident.
- Évaluez votre processus d'intervention en cas d'incident et faites ressortir les éléments à améliorer.
- Tenez une réunion avec votre équipe d'intervention et rédigez un document sur les leçons apprises et les mesures à prendre pour améliorer le processus.

Servez-vous de ces quatre étapes pour structurer votre plan et votre intervention. Au moment de mettre votre plan à exécution, vous devriez d'abord signaler le cybercrime :

- au service de police local;

- en ligne au Centre antifraude du Canada;
- en ligne au Centre pour la cybersécurité.

Élaborer un plan de reprise

Votre plan de reprise devrait venir appuyer votre plan de sauvegarde et vos plans d'intervention en cas d'incident. Lors de l'élaboration de votre plan de reprise, tenez compte de nombreux facteurs, en plus de définir et de documenter clairement ce qui doit être récupéré, par qui, quand et où.

Lignes directrices pour le plan de reprise

Consultez les lignes directrices suivantes quant à votre plan de reprise.

Planification

- Indiquez toutes les parties prenantes, notamment la clientèle, les fournisseurs, les propriétaires d'entreprise, les propriétaires de systèmes et les gestionnaires.
- Indiquez les membres de votre équipe d'intervention, et leurs rôles et responsabilités.
- Faites l'inventaire de vos biens matériels et logiciels.
- Déterminez les fonctions, les applications et les données opérationnelles qui sont essentielles et classez-les par ordre de priorité.
- Préparez des documents sur les situations d'urgence, dont une liste de personnes-ressources, qui seront distribués au personnel, à la clientèle, aux fournisseurs de services et à d'autres fournisseurs, pour que vous puissiez intervenir rapidement et efficacement en cas d'incident lié à un rançongiciel.
- Dirigez un exercice sur table pour vous assurer que les participantes et participants connaissent leur rôle et les mesures d'intervention à prendre en cas d'attaque par rançongiciel.
- Investissez dans une police d'assurance en matière de cybersécurité si vous jugez que cela pourrait être bénéfique pour votre organisation. Elle peut ajouter une couche de protection supplémentaire, en plus d'offrir à votre organisation une expertise en matière d'intervention en cas d'incident dans l'éventualité d'une attaque par rançongiciel.

Évaluation

- Fixez des objectifs de reprise clairs.
- Définissez des stratégies de sauvegarde et de récupération des données.

- Mettez votre plan à l'essai.

Communication

- Élaborez un plan de communications pour informer les principales parties prenantes.
- Élaborez un programme de formation à l'intention des employées et employés afin de vous assurer qu'ils comprennent leurs rôles, leurs responsabilités et le déroulement des opérations pendant un incident.
- Discutez avec vos FSG pour déterminer les façons dont ils peuvent appuyer vos efforts de reprise.
- Faites appel à des spécialistes de la sécurité des TI avant qu'un événement se produise pour bien vous entourer de spécialistes en la matière aptes à donner son avis sur vos efforts en matière d'intervention et de reprise.

Pour élaborer un plan efficace, vous devez déterminer les données, les applications et les fonctions organisationnelles qui sont essentielles. Parmi les données essentielles, on peut retrouver des dossiers financiers, des actifs exclusifs et des renseignements personnels. Quant aux applications essentielles, ce sont les systèmes qui exécutent les principales fonctions qui sont indispensables à votre entreprise. Vous devrez restaurer immédiatement les données, les applications et les fonctions essentielles pour assurer la continuité des activités en cas de panne ou d'incident imprévu. Vous devriez envisager la possibilité de faire une évaluation des risques pour aider à déterminer les fonctions opérationnelles essentielles ainsi que les risques pertinents liés aux menaces et aux vulnérabilités.

Pour assurer une intervention efficace, votre organisation devra revoir certains scénarios précis, comme une cyberattaque, une panne de courant importante ou une catastrophe naturelle. Ainsi, vous serez en mesure de déterminer les principaux intervenants et les parties prenantes, à gérer les risques importants, à élaborer des stratégies d'atténuation et à déterminer le temps et les efforts nécessaires à la reprise des activités.

Vous pouvez mener une analyse des répercussions sur les activités (ARA) pour prévoir les répercussions d'une interruption ou d'un incident sur vos opérations, vos processus opérationnels, vos systèmes et vos finances. Il faudra que presque tous les processus de reprise soient sans connexion à Internet pendant une longue période afin d'expulser les auteurs. Prévoyez d'inclure cette période d'indisponibilité dans votre ARA.

Dans cette analyse, vous devrez également évaluer les données que vous recueillez et les applications que vous utilisez pour déterminer leur criticité et établir les priorités qui permettront une

reprise immédiate. Il est aussi important de prendre note des efforts déployés en matière de reprise, en documentant ce qui s'est bien passé et en précisant les points à améliorer.

Pour en apprendre davantage sur l'élaboration de votre plan de reprise, consultez la publication Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004).

Gérer les comptes d'utilisateur et d'administrateur

Supervisez la création et l'attribution de comptes d'administrateur et d'utilisateur en gardant à l'esprit l'accès sécurisé. Envisagez la création de comptes distincts pour des fonctions non administratives (par exemple, un accès au courriel et un accès limité aux systèmes internes) afin de réduire le risque qu'un rançongiciel infecte vos comptes d'administrateur et l'accès au système associé à ces comptes. Vous devez limiter les comptes d'administrateur aux personnes qui ont besoin d'un accès complet ou d'un accès spécialisé au réseau, aux systèmes et aux dispositifs de votre organisation. Assurez-vous d'avoir une séparation complète des tâches pour le personnel d'administration suppléant par rapport au personnel d'administration principal et de production. Portez une attention particulière aux systèmes de gestion des autorisations communs ou fédérés possibles, comme les services d'annuaire ou les fournisseurs d'identité en nuage.

Votre organisation devrait utiliser des postes de travail administratifs spécialisés afin de créer des environnements sécurisés exclusivement pour les opérations privilégiées. Le retrait de l'accès Internet public des postes de travail administratifs peut considérablement réduire les risques de compromission. L'accès à distance à des comptes privilégiés devrait s'effectuer à partir de postes de travail administratifs spécialisés régis entièrement par les stratégies de sécurité du système et utilisées exclusivement à cette fin.

Si un auteur de menace obtient l'accès à un compte d'administrateur, il peut utiliser les privilèges élevés pour nuire à l'environnement opérationnel de votre organisation, attaquer votre réseau ou accéder à de l'information sensible. Les auteurs de menace peuvent aussi découvrir quels mécanismes de détection et de reprise existent sur vos systèmes, ce qui pourrait les aider à les contourner et vous empêcher de prévenir d'autres attaques.

Pour gérer l'accès à vos systèmes et données, appliquez le principe de droit d'accès minimal. Autrement dit, ne donnez au personnel que l'accès aux fonctions et aux privilèges dont il a besoin pour réaliser son travail. Vous devriez également utiliser ce principe pour accorder un accès à distance à vos appareils. Assurez-vous d'activer l'AMF pour tous les points d'accès menant à votre réseau. Envisagez le recours à un accès à authentification unique, si possible, pour renforcer la sécurité de vos dispositifs et de vos réseaux connectés. Restreignez les privilèges administratifs et

exigez une confirmation pour chaque action qui nécessite des droits d'accès et des autorisations de niveau élevé.

Votre organisme doit prendre les mesures suivantes lorsqu'il assigne des comptes d'administrateur ou des privilèges d'accès aux utilisatrices et utilisateurs :

- Utiliser des méthodes d'authentification robustes pour les comptes :
  - Recourir à l'AMF pour tous les comptes d'administrateur.
  - Utiliser une phrase de passe unique pour chaque compte privilégié.
  - Remplacer les mots de passe par défaut par des phrases de passe uniques pour les applications et les dispositifs.
  - Authentifier les utilisatrices et utilisateurs avant qu'ils obtiennent l'accès aux applications ou aux dispositifs.
- Veiller à ce que des comptes uniques et identifiables soient remis à chaque utilisatrice ou utilisateur.
- Consigner et surveiller les activités effectuées sur les comptes privilégiés.
- Offrir de la formation sur les comportements attendus aux utilisatrices et utilisateurs de comptes privilégiés.
- Retirer les privilèges d'accès spécial dès que les utilisatrices et utilisateurs n'en ont plus besoin.
- Désactiver et supprimer les comptes d'utilisateur lorsque quelqu'un quitte l'organisation.

Pour relever les défis d'aujourd'hui liés à la sécurisation du personnel travaillant à distance, aux environnements infonuagiques hybrides et aux menaces pour la cybersécurité, il est recommandé de mettre en œuvre un modèle de sécurité à vérification systématique (MVS). Le principe central du MVS veut qu'aucun élément (application, utilisateur ou appareil) d'un système d'information ne soit digne de confiance par défaut. Il faut réévaluer et vérifier la confiance chaque fois qu'un élément demande l'accès à une nouvelle ressource. Le niveau d'accès accordé est rajusté de manière dynamique en fonction du degré de confiance établi pour l'élément. Le MVS consiste à adopter une nouvelle façon de voir la sécurité en anticipant toujours une atteinte à la sécurité et en accordant la priorité à la protection des ressources (par exemple, les services et les données). Pour en savoir plus sur les MVS, consultez la publication Approche à vérification systématique pour l'architecture de sécurité (ITSM.10.008). Outre la gestion de vos comptes, il est aussi impératif de gérer la mise hors service et la déconnexion de systèmes et de dispositifs désuets ou qui ne sont plus utilisés. Ces

systèmes et dispositifs doivent être retirés de votre réseau, leur contenu doit être expurgé et ils doivent être éliminés de manière sécurisée.

Pour obtenir de plus amples renseignements sur la gestion de l'accès et des comptes d'administateur, consultez les publications suivantes :

- Gestion et contrôle des privilèges d'administrateur (ITSM.10.094)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)

Contrôles de cybersécurité

Dans le cadre de la mise en œuvre et de la tenue à jour d'un modèle de défense en profondeur, votre organisation doit appliquer plusieurs couches de contrôles de sécurité dans l'ensemble des réseaux pour ainsi protéger la sécurité, la confidentialité, l'intégrité et la disponibilité de vos réseaux, de vos dispositifs et de vos renseignements.

Ainsi que le montre la figure 2 ci-dessous, divers contrôles de sécurité, mis en place à plusieurs niveaux de vos réseaux, permettent de mieux défendre l'organisation contre les rançongiciels. Certains des contrôles de cybersécurité indiqués à la figure 2 peuvent être appliqués à différentes étapes ou dans différentes zones de votre réseau et de vos systèmes. À titre d'exemple, il conviendrait d'appliquer les mécanismes de journalisation, d'alerte et de segmentation de réseau à tous les niveaux de votre stratégie de défense en profondeur.
Pour atténuer de façon proactive les menaces durant la première étape d'un incident lié à un rançongiciel, il est essentiel de mettre en place des mesures préventives et des contrôles de cybersécurité clés avant qu'un incident se produise. En appliquant les contrôles suivants dans votre environnement de sécurité, vous pouvez renforcer la capacité de votre organisation à détecter, à endiguer et à réduire d'emblée l'incidence des menaces de rançongiciel.

- Donnez à vos employées et employés une formation personnalisée sur la cybersécurité pour qu'ils soient bien au courant des vecteurs d'attaque, comme l'hameçonnage, et qu'ils sachent comment détecter les courriels ou les liens suspects.
- Utilisez des phrases de passe robustes pour prévenir les attaques liées à l'authentification.
- Appliquez l'AMF pour sécuriser les dispositifs et les systèmes de votre organisation.
- Créez une liste d'applications autorisées pour contrôler qui ou quoi est autorisé à accéder à vos réseaux et à vos systèmes. Les listes d'applications autorisées permettent d'éviter le téléchargement d'applications malveillantes qui pourraient infecter votre serveur.

- Analysez votre matériel, vos logiciels et votre système d'exploitation pour détecter des vulnérabilités. Appliquez des correctifs et des mises à jour afin d'atténuer le risque que les vulnérabilités soient exploitées par un auteur de menace.
- Segmentez votre réseau pour vous assurer que l'information sensible et de grande valeur se trouve dans une zone distincte de votre réseau.
- Configurez des fonctions de surveillance et de journalisation pour vos systèmes et réseaux, et assurez-vous de recevoir des alertes automatisées en cas de détection d'anomalies.
- Protégez vos systèmes connectés ou exposés à Internet par les moyens suivants :
    - le chiffrement;
    - les pare-feu;
    - les SDPI;
    - des évaluations des vulnérabilités fréquentes.
- Désactivez les macros pour réduire le risque de propagation des rançongiciels par des pièces jointes et veillez à ce que les utilisatrices et utilisateurs ne puissent pas les réactiver.
- Bloquer les publicités, en particulier les publicités malveillantes, pour empêcher qu'elles soient affichées.

Pour atténuer les menaces survenant au cours de la deuxième étape d'un incident lié à un rançongiciel, vous pouvez prendre les mesures suivantes en vue de mieux protéger vos systèmes et vos réseaux et pour empêcher la propagation des rançongiciels dans votre réseau et vos dispositifs connectés :

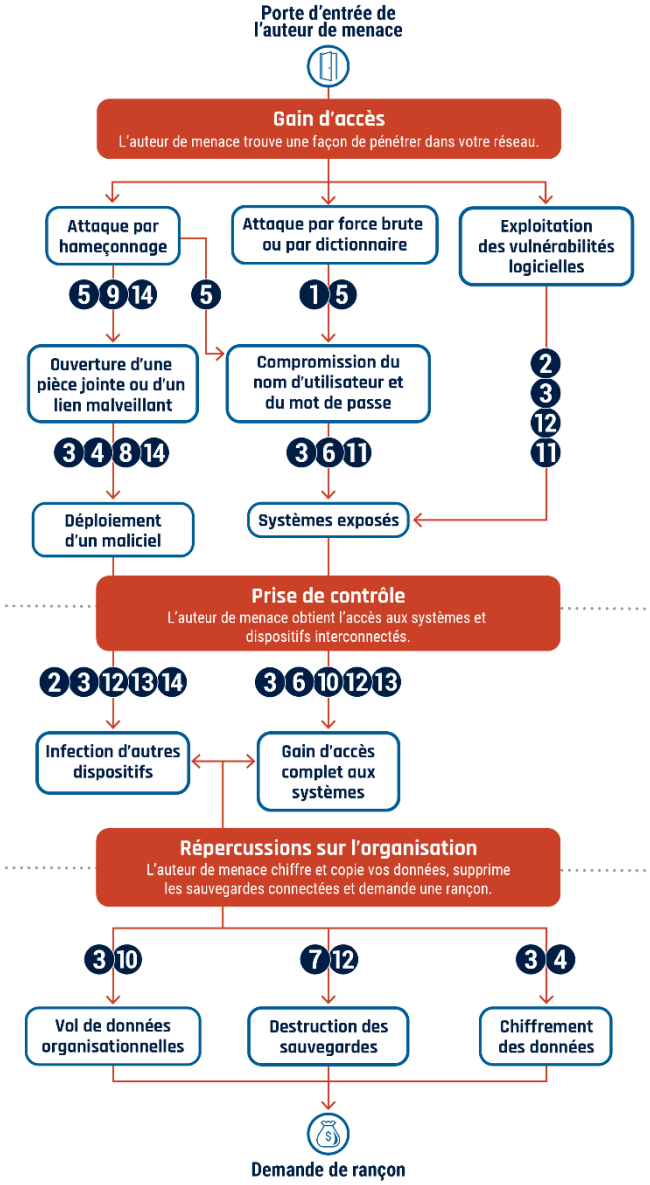
- Utilisez des outils de sécurité, comme les antivirus et les antimaliciels.
- Utilisez des pare-feu et un SDPI sur vos réseaux pour protéger les points d'entrée potentiels contre les auteurs de menace.
- Appliquez le principe du droit d'accès minimal.

Lors de la troisième étape d'un incident lié à un rançongiciel, la plus importante mesure d'atténuation pour votre organisation est son plan de sauvegarde. Assurez-vous de stocker plusieurs copies de vos sauvegardes hors ligne. Lorsque vos sauvegardes sont déconnectées de tous les réseaux, il sera plus difficile pour les auteurs de menace ayant recours à un réseau de les supprimer ou de les infecter d'un rançongiciel. Assurez-vous de tester régulièrement vos processus de sauvegarde et de restauration. Réglez tout problème immédiatement pour vous assurer que vos fichiers de sauvegarde sont prêts à être récupérés rapidement par votre organisation en cas d'incident lié à un rançongiciel.

La section suivante présente des indications plus détaillées sur les divers contrôles de sécurité que votre organisation peut mettre en œuvre. Pour en savoir plus sur les contrôles de sécurité, consultez les publications suivantes :

- Contrôles de cybersécurité de base pour les petites et moyennes organisations
- Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises (ITSAP.10.035)

Figure 2: Contrôles de sécurité pour réduire le risque d'incident lié au rançongiciel



Description longue – Figure 2 : Contrôles de sécurité pour réduire le risque d'incident lié au rançongiciel

La figure 2 montre la même méthodologie qu'utilise un auteur de menace pour mener une attaque par rançongiciel, mais elle met en relief les endroits où des contrôles de sécurité peuvent être mis en œuvre afin d'atténuer la menace et de tenter d'empêcher que se produise une attaque par rançongiciel.

Dans la première étape d'un incident lié à un rançongiciel, sous la section « Gain d'accès » du présent schéma, certaines mesures préventives d'atténuation peuvent être mises en place pour protéger votre organisation. Voici une liste des contrôles de cybersécurité pouvant être mis en œuvre au premier plan de votre environnement de cybersécurité :

- Donnez à vos employées et employés une formation personnalisée sur la cybersécurité pour qu'ils soient bien au courant des vecteurs d'attaque, comme l'hameçonnage, et qu'ils sachent comment détecter les courriels ou les liens suspects.
- Utilisez des mots de passe forts, ou de préférence des phrases de passe, pour empêcher les auteurs de menace de mener des attaques par force brute.
- Appliquez l'AMF pour sécuriser les dispositifs de votre organisation.
- Créez une liste d'applications autorisées pour contrôler qui ou quoi est autorisé à accéder à vos réseaux et à vos systèmes. Les listes d'applications autorisées permettent d'éviter le téléchargement d'applications malveillantes qui pourraient infecter votre serveur.
- Analysez votre matériel, vos logiciels et votre système d'exploitation pour détecter des vulnérabilités. Appliquez des correctifs et des mises à jour afin d'atténuer le risque que les vulnérabilités soient exploitées par un auteur de menace.
- Segmentez votre réseau pour vous assurer que l'information sensible et de grande valeur se trouve dans une zone différente de votre réseau.
- Configurez des fonctions de surveillance et de journalisation pour vos systèmes et réseaux, et assurez-vous de recevoir des alertes automatisées en cas de détection d'anomalies.
- Protégez vos systèmes connectés ou exposés à Internet par les moyens suivants :
    - le chiffrement;
    - les pare-feu;
    - l'AMF;
    - des évaluations des vulnérabilités fréquentes.

- Désactivez les macros pour diminuer le risque de propagation des rançongiciels par des pièces jointes de Microsoft Office.

Dans la deuxième étape d'un incident lié à un rançongiciel, sous la section « Prise de contrôle » du présent schéma, certaines mesures d'atténuation peuvent être mises en place pour mieux protéger vos systèmes et vos réseaux et empêcher la propagation des rançongiciels dans votre réseau et vos dispositifs connectés.

- Mettez en œuvre des outils de sécurité dans vos réseaux, comme un antivirus, un antimaliciel et des pare-feu, pour ajouter des couches de protection aux points d'entrée que pourraient utiliser les auteurs de menace.
- Appliquez le principe du droit d'accès minimal selon lequel il convient de n'accorder aux personnes que les privilèges d'accès dont elles ont besoin pour effectuer les tâches qui leur sont autorisées.

Lors de la troisième étape d'un incident lié à un rançongiciel, sous la section « Répercussions sur l'organisation », la plus importante mesure d'atténuation que vous pouvez mettre en œuvre pour votre organisation est votre plan de sauvegarde. Assurez-vous de stocker plusieurs copies de vos sauvegardes hors ligne et, si possible, dans le nuage par l'entremise d'un FSI. Lorsque vos sauvegardes sont déconnectées de votre réseau, les auteurs de menace sont incapables de les supprimer ou de les infecter d'un rançongiciel. Assurez-vous de tester souvent vos processus de sauvegarde et de rétablissement et faites immédiatement les ajustements nécessaires pour faire en sorte que vos fichiers de sauvegarde sont prêts pour que votre organisation puisse se remettre rapidement en cas d'incident lié à un rançongiciel.

Créer une liste d'applications autorisées

La liste d'applications autorisées est un portefeuille de logiciels approuvés. La liste permet de faire en sorte que seuls les logiciels approuvés soient installés dans les divers systèmes d'une organisation. Une liste d'applications autorisées permet de sélectionner et d'établir les applications et les composants d'applications (par exemple, programmes exécutables, bibliothèques de logiciels ou fichiers de configuration) qui sont autorisés à s'exécuter sur des systèmes organisationnels. Les listes d'applications autorisées permettent d'éviter le téléchargement et l'infection d'applications malveillantes sur votre serveur.

Votre organisation peut créer une liste des applications dont l'utilisation est autorisée dans les lieux de travail ou qui proviennent d'un fournisseur digne de confiance. Lorsqu'une application est lancée, elle est comparée à la liste d'applications autorisées et n'est permise que si elle figure sur la liste. Le

hachage sert à vérifier l'intégrité de l'application et génère une valeur à partir d'une chaîne de textes qui est unique pour chaque application. Si une application est mise à jour ou a été corrigée, le hachage change pour vous permettre d'exécuter uniquement la plus récente version de l'application. Une mesure complémentaire à l'établissement d'une liste d'applications autorisées consiste à imposer le recours aux signatures de fournisseurs de logiciels approuvés pour tous les types de logiciels.

En mettant en œuvre une liste d'applications autorisées, votre organisation sera en mesure de renforcer sa posture de cyberdéfense et de prévenir des incidents comme ceux liés aux rançongiciels.

Pour obtenir de plus amples renseignements sur les listes d'applications autorisées, consultez la publication Mettre en place une liste d'applications autorisées (ITSM.10.095).

Utiliser un système d'adressage par domaine de protection

Un système d'adressage par domaine (DNS pour *Domain Name System*) est un protocole qui met en correspondance les noms de domaine lisibles par l'humain et les adresses IP lisibles par la machine. On l'appelle souvent le carnet d'adresses d'Internet. Le DNS est utilisé à la fois pour les actions lancées par l'humain (par exemple, consulter un site Web) et pour celles lancées par la machine (par exemple, exécuter une mise à jour).

Le DNS de protection est un outil que votre organisation peut utiliser pour bloquer l'accès des dispositifs organisationnels des employées et employés à des domaines potentiellement malveillants sur Internet. Il détecte les domaines malveillants en les comparant à la liste de blocage de votre organisation, laquelle comprend les domaines et adresses IP qu'il est interdit de consulter sur le réseau organisationnel ou au moyen de biens organisationnels. Pour en savoir plus sur le DNS, consultez les publications Système d'adressage par domaine de protection (ITSAP.40.019) et Trafiquage du service de noms de domaine (DNS) (ITSAP.40.021).

Vous devriez également envisager d'installer un filtre DNS de protection sur les appareils mobiles qu'utilisent les employées et employés, surtout s'ils peuvent se connecter à vos systèmes et à votre réseau à distance. Pour ce faire, vous pouvez configurer manuellement les paramètres DNS sur les appareils de votre organisation, à l'aide d'un outil de gestion des postes mobiles (MDM pour *Mobile Device Management*). Pour de plus amples renseignements sur la protection des appareils mobiles, consultez la publication Facteurs relatifs à la sécurité à considérer pour les dispositifs d'accès (ITSM.80.101).

Les Canadiennes et Canadiens peuvent se servir du Bouclier canadien, une application DNS publique gratuite. L'application, offerte par l'Autorité canadienne pour les enregistrements Internet (ACEI), permet de veiller à ce que les appareils personnels utilisent toujours un DNS fiable qui filtre les adresses IP malveillantes. Le Bouclier canadien peut être configuré sur votre routeur ou votre passerelle afin d'assurer une meilleure protection de l'ensemble de votre réseau. Il est recommandé d'appliquer le résolveur DNS protégé de l'ACEI, lequel est conçu pour permettre le blocage efficace des maliciels et des tentatives d'hameçonnage. En remplaçant les paramètres par défaut du serveur DNS sur vos dispositifs par un serveur DNS fiable, vos appareils seront mieux protégés.

Établir un système de défense périphérique

La protection de votre réseau et de vos systèmes et dispositifs connectés contre les cybermenaces peut paraître complexe à réaliser. Le périmètre de défense protège la frontière entre deux zones de sécurité de réseau à travers laquelle le trafic est acheminé. La défense de cette frontière en recourant à des protocoles de sécurité de base, comme des pare-feu, un antivirus, un antimaliciel ou un SDPI renforce considérablement votre protection globale. L'installation d'un logiciel antihameçonnage est aussi une façon de renforcer la cybersécurité de votre organisation. Les logiciels antihameçonnage bloquent les courriels d'hameçonnage dans le but de prévenir les attaques et leur propagation.

Assurez-vous que les utilisatrices et utilisateurs accèdent au réseau au moyen du réseau privé virtuel (RPV) de votre organisation. Le RPV sert de tunnel sécurisé par l'entremise duquel on peut envoyer et recevoir des données dans un réseau physique existant. L'utilisation d'un RPV assure une connexion sécurisée entre deux points, comme un ordinateur portable et le réseau d'une organisation.

Mettre en œuvre un mécanisme de journalisation et d'alerte

La mise en œuvre d'une surveillance continue de vos réseaux vous aidera à établir les profils d'activité acceptables de référence au sein de votre organisation. L'établissement de capacités de surveillance, comme des systèmes de détection d'intrusion (SDI) pour vos réseaux, peut aider votre organisation à gérer les risques. Votre système de surveillance devrait générer des journaux que les spécialistes en TI et la direction peuvent examiner au besoin. Vous devriez limiter l'accès aux journaux aux personnes qui ont besoin de les examiner.

Vous devriez également intégrer un mécanisme d'alerte automatique à vos capacités de surveillance pour que les anomalies dans les tendances dans les profils d'activité soient signalées et examinées. Le mécanisme d'alerte automatique devrait également permettre de repérer les vulnérabilités et les événements potentiels qui vous obligent à prendre des mesures d'atténuation des risques. Les

alertes indiqueront toute activité hors de l'ordinaire qui a eu lieu. Votre organisation peut ensuite examiner l'anomalie pour établir ce qui s'est passé, si elle présente un risque pour l'organisation et les mesures pouvant être prises pour atténuer le risque. Le système de journalisation et d'alerte de votre organisation ne devrait pas permettre la modification des journaux une fois que ceux-ci ont été reçus du système. Les journaux devraient porter une estampille temporelle afin de vous aider à comprendre les circonstances de l'événement ou de l'incident.

Si votre organisation est victime d'une attaque par rançongiciel ou de tout autre type de cyberincident, vos journaux pourraient vous fournir de l'information sur la façon dont s'est déroulé l'incident. Ils pourraient également montrer les contrôles ou mesures d'atténuation pouvant être appliqués pour mieux protéger vos réseaux et systèmes et ainsi éviter d'autres incidents.

Pour de plus amples renseignements sur la mise en œuvre d'un mécanisme de journalisation et d'alerte, consultez la publication Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085).

Évaluer les vulnérabilités

Une évaluation des vulnérabilités peut permettre de repérer les vulnérabilités connues que les cybercriminelles et cybercriminels pourraient exploiter pour avoir accès aux applications, aux systèmes et aux données, et d'y remédier. Cette évaluation peut comprendre ce qui suit :

- une analyse des vulnérabilités pour repérer les vulnérabilités connues dans des applications;
- des tests d'intrusion, qui simulent des attaques que les cybercriminelles et cybercriminels pourraient mener pour évaluer la capacité de l'infrastructure à y résister;
- des évaluations et contrôles de sécurité pour repérer les mauvaises configurations qui pourraient engendrer des vulnérabilités informatiques;
- la détection d'intrusion pour surveiller les intrusions et les tentatives d'intrusion;
- la chasse aux cybermenaces pour repérer et éliminer les menaces au moyen de la criminalistique informatique, du renseignement sur les cybermenaces et de l'analyse de maliciels.

Segmenter les réseaux

La segmentation de votre réseau consiste à diviser vos réseaux en petites sections ou zones afin que le trafic soit dirigé et qu'il circule dans les différentes sections du réseau. Cela vous permet de suspendre le flux du trafic dans certaines zones et de l'empêcher de passer dans d'autres secteurs

de votre réseau. De même, la segmentation vous permet aussi d'isoler et d'arrêter la propagation de maliciels dans différentes sections de votre réseau, et de contrôler et de restreindre l'accès à vos renseignements. Lors de la segmentation de votre réseau, assurez-vous que les réseaux de TI et de technologies opérationnelles (TO) sont définis, séparés et surveillés. Ces réseaux devraient être isolés, ce qui signifie que vous devriez isoler physiquement ou conceptuellement les réseaux informatiques sécurisés des réseaux non sécurisés, comme ceux qui se connectent à Internet. Outre la segmentation de vos réseaux TI et TO, vous devez également détecter les interdépendances entre ceux-ci et mettre en œuvre des mesures à appliquer durant un cyberincident afin de protéger les fonctions et les données essentielles.

Pour en savoir plus sur la segmentation de réseaux, consultez la publication Segmenter et séparer l'information (ITSM.10.092).

Limiter les environnements de développement et de scripts et désactiver les macros

Si votre organisation utilise le système d'exploitation Microsoft Windows, vous pourriez vouloir envisager de limiter vos environnements de développement et de scripts. Spécifiquement pour une utilisation Windows, Microsoft a conçu une application automatisée d'administration système par l'entremise d'une interface optimisée par le langage de script de son interpréteur de ligne de commande (connu sous le nom PowerShell). Il s'agit d'une partie très importante de la boîte à outils d'administration système. L'application peut être utilisée pour contrôler entièrement les systèmes Windows de Microsoft, et elle apporte de nombreux avantages aux organisations. Toutefois, les auteurs de menace peuvent exploiter PowerShell et injecter du code malveillant dans la mémoire de vos dispositifs. Le plus inquiétant, c'est que PowerShell est une source fiable. Par conséquent, l'antivirus ou l'antimaliciel ne bloquera généralement pas l'injection de code malveillant, et les journaux d'événement de vos systèmes ne signaleront pas d'anomalie. Pour que les comportements malveillants de PowerShell soient plus difficiles à masquer, les organisations devraient s'assurer que les utilisatrices et utilisateurs standards sont autorisés à modifier les clés de registre ou le dossier de transcription pertinents.

Les organisations devraient également envisager d'utiliser un mécanisme de journalisation d'événements protégé pour empêcher la fuite de renseignements sensibles, comme des mots de passe dans des blocs de script qui sont enregistrés dans le journal d'événements.

De nombreuses organisations disposent également d'outils de développement, comme Python, Perl, PHP et .NET, que les auteurs de menace peuvent exploiter à des fins malveillantes. Isolez ces outils de l'environnement utilisateur.

Les macros sont un autre facteur relatif à la sécurité à considérer lorsque vous utilisez Windows. Les macros sont des séquences écrites qui imitent les frappes et les commandes de souris des utilisateurs pour automatiquement répéter les tâches dans les applications. Les macros sont utilisées dans de nombreux produits Microsoft Office pour automatiser les processus et les flux de données. Elles sont intégrées au code des fichiers, ce qui permet aux utilisatrices et utilisateurs de créer des raccourcis pour des tâches précises (par exemple, trier des feuilles de travail par ordre alphabétique, défusionner toutes les cellules fusionnées, afficher toutes les rangées et les colonnes cachées).

Les auteurs de menace peuvent créer des macros malveillantes et les intégrer dans des documents qu'ils peuvent ensuite envoyer à des employés de votre organisation. Afin de réduire le risque qu'un rançongiciel se propage par l'entremise de pièces jointes Office, il est recommandé de régler les valeurs implicites utilisateur de façon à désactiver les macros et de s'assurer que les utilisatrices et utilisateurs ne sont pas en mesure de les réactiver. Vous devez également vous assurer que les macros ne contiennent pas de renseignements sensibles, comme des justificatifs personnels, et utiliser des macros signées ou créées par l'organisation, et qui ont été vérifiées par les responsables techniques de votre organisation.

Pour obtenir de plus amples renseignements sur les macros, consultez la publication Protection d'un organisme contre les macros malveillantes (ITSAP.00.200).

Appliquer les correctifs et mises à jour

Pour protéger vos dispositifs connectés contre les rançongiciels, vérifiez régulièrement si de nouvelles mises à jour sont offertes pour le système d'exploitation, les logiciels et le micrologiciel, et installez les correctifs de sécurité nécessaires. Il existe divers correctifs sur le marché, mais les trois types suivants sont les plus répandus :

- Correctif : Règle les problèmes liés aux fonctionnalités des logiciels (par exemple, une erreur qui amène un dispositif à réagir de façon inattendue);
- Correctif de sécurité : Compense les vulnérabilités dans le but de protéger le système contre les menaces (par exemple, un maliciel qui infecte les dispositifs suivant l'exploitation de vulnérabilités);
- Mise à jour des fonctions : Ajoute de nouvelles fonctions à un logiciel déjà installé (par exemple, une amélioration du rendement ou de la rapidité de traitement d'une application).

Pour en savoir plus sur l'application des correctifs et de mises à jour, consultez la publication Appliquer les correctifs aux systèmes d'exploitation et aux applications (ITSM.10.096).

Gérer les mots de passe et les phrases de passe

Votre organisation devrait mettre en œuvre des phrases de passe au lieu de mots de passe, si possible. Le recours à des phrases de passe robustes est un bon moyen de protection, mais il ne permet pas à lui seul d'empêcher les auteurs de menace d'accéder à vos systèmes et à votre information sensible. Une attaque par dictionnaire est une tactique courante qu'emploient les auteurs de menace pour pénétrer dans vos systèmes et réseaux. S'il n'est pas possible d'utiliser des phrases de passe, optez pour des mots de passe uniques et robustes combinés à l'AMF.

La sous-section Gérer les comptes d'utilisateur et d'administrateur contient de plus amples détails sur l'adoption de l'AMF dans vos pratiques de gestion de l'accès et des comptes. Parallèlement à l'AMF, vous devriez encourager les employées et employés à utiliser un gestionnaire de mots de passe. Un gestionnaire de mots de passe peut permettre de se souvenir des mots de passe ou phrases de passe système et réseau, et de les sécuriser.

En outre, votre organisation devrait considérer la mise en œuvre de coffres-forts de mots de passe pour les comptes administratifs. Ces coffres-forts procurent un niveau supérieur de protection, puisque les mots de passe ou phrases de passe sont soumis à des cycles et sont synchronisés avec vos systèmes. Ainsi, une phrase de passe ou un mot de passe ne peut être utilisé qu'une seule fois. Il peut être retracé de manière à déterminer qui a utilisé le mot de passe ou la phrase de passe, quand et pour accéder à quoi.

Pour obtenir plus d'information sur la mise en œuvre et l'utilisation des gestionnaires de mots de passe, consultez les publications Conseils de sécurité sur les gestionnaires de mots de passe (ITSAP.30.025) et Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032).

Protéger les domaines de courriel

Les auteurs de menace peuvent tirer avantage de mauvaises configurations ou de lacunes dans les protocoles de cybersécurité pour atteindre leurs objectifs. Ils ciblent souvent des systèmes de courrier électronique dans le but d'obtenir un accès non autorisé, de voler de l'information sensible ou de perturber les canaux de communication. Les comptes de courrier électronique hébergent une grande quantité de renseignements particuliers, dont des données personnelles, des renseignements financiers et des échanges commerciaux confidentiels. Il est donc important de bien sécuriser les

communications par courriel pour prévenir les intrusions qui risquent de compromettre l'intégrité des échanges. La sécurité du courrier électronique offre également une protection contre les attaques par maliciel et par hameçonnage, qui sont souvent amorcées au moyen de courriels trompeurs.

Évaluez la possibilité de mettre en œuvre des mesures de sécurité techniques pour repérer l'infrastructure utilisée par les auteurs de menace, protéger les domaines de votre organisation contre l'usurpation d'adresses électroniques et empêcher la réception de messages malveillants envoyés frauduleusement au nom de votre domaine. Ces mesures vous permettront également de bloquer les courriels d'hameçonnage envoyés à votre organisation. Vous pouvez réduire les risques liés aux campagnes d'envoi de courriels malveillants en appliquant les trois protocoles de sécurité suivants qui agissent conjointement pour empêcher l'usurpation des domaines de courriel. Pour en savoir plus, consultez la publication Guide rapide sur la configuration du courrier électronique (ITSAP.60.003).

Protocole SPF

Le protocole SPF (*Sender Policy Framework*) est un système qui utilise des fonctions du DNS et qui permet aux propriétaires de domaines de spécifier les serveurs qui sont autorisés à envoyer des courriels au nom du domaine. Si vous recevez un courriel provenant d'une adresse IP qui n'est pas explicitement autorisée et répertoriée dans l'enregistrement SPF, il n'est probablement pas légitime. Ainsi, lorsqu'un courriel est envoyé, le serveur de courrier électronique de la ou du destinataire consulte l'enregistrement SPF du domaine de l'expéditrice ou expéditeur afin de vérifier si le serveur de courrier électronique de ce dernier figure sur la liste d'autorisation. Si le serveur de courrier électronique de l'expéditrice ou expéditeur figure dans l'enregistrement SPF (réussite de l'envoi), le courriel est considéré comme légitime et est normalement livré comme il se doit. Toutefois, si le serveur de courrier électronique de l'expéditrice ou expéditeur ne figure pas dans l'enregistrement SPF (échec de l'envoi), le serveur de courrier électronique de la ou du destinataire traitera le courriel avec prudence et pourrait le rejeter ou le classer dans le courrier indésirable.

Protocole DKIM

Le protocole DKIM (*DomainKeys Identified Mail*) est un mécanisme d'authentification du courrier électronique qui renforce la sécurité des courriels en permettant à l'expéditrice ou expéditeur de signer numériquement les courriels. Lorsqu'un système de courrier électronique qui prend en charge le protocole DKIM reçoit un message comportant une signature DKIM, il récupère l'enregistrement associé à l'en-tête DKIM du message et vérifie la signature à l'aide de la clé publique publiée. Cette

vérification confirme sur le plan cryptographique que le message a été envoyé par un expéditeur autorisé et qu'il n'a pas été modifié pendant sa transmission. Si la signature n'est pas valide ou si aucun enregistrement DKIM n'est trouvé, le message échouera à la vérification DKIM. Le message qui ne répondra pas aux critères de vérification DKIM pourrait être rejeté.

Le protocole DKIM permet ainsi d'assurer l'intégrité des communications par courriel, sans altération des messages. Les serveurs des destinataires doivent vérifier l'authenticité du message et confirmer que celui-ci provient du domaine indiqué. Cela permet de prévenir les tentatives d'usurpation d'identité et d'adresse électronique.

Protocole DMARC

La mise en œuvre d'une politique et d'une vérification du protocole DMARC (*Domain-based Messaged Authentication, Reporting and Conformance*) peut renforcer vos protocoles de sécurité et empêcher l'usurpation de votre domaine de courriel. Il exploite les protocoles DKIM et SPF pour s'assurer que les courriels sont authentifiés avant la transmission, garantissant que les courriels proviennent du domaine prévu et qu'ils sont expédiés à des destinataires légitimes. Si un courriel passe par la validation DMARC, il sera acheminé à la ou au destinataire prévu. Toutefois, si le courriel échoue à la validation DMARC, le système de courriel récepteur applique la politique précisée dans l'enregistrement DMARC du domaine, puis il choisira alors d'acheminer le courriel, de l'acheminer, mais en le marquant comme suspect, ou de le rejeter. Contrairement à d'autres solutions qui reposent sur un point de défaillance unique, le protocole DMARC emploie une stratégie résiliente couvrant à la fois les côtés source et cible des communications par courriel. Il assure une vérification de sécurité complète de l'information de l'expéditrice ou expéditeur, des détails de la ou du destinataire, de la ligne d'objet, du contenu textuel et d'autres caractéristiques du message.
Pour obtenir de plus amples renseignements sur la protection des domaines de courriel, consultez les publications Directives de mise en œuvre – protection du domaine de courrier (ITSP.40.065) et Pratiques exemplaires en matière de sécurité pour le courrier électronique (ITSM.60.002).

Se remettre d'un incident lié à un rançongiciel

Se remettre d'un incident lié à un rançongiciel peut s'avérer un long processus, et rétablir la marque et la réputation de votre organisation peut prendre encore plus de temps. Travailler dans l'optique que votre organisation devra inévitablement faire face à des maliciels peut vous aider à élaborer un plan d'intervention et pourrait vous permettre d'accélérer le temps de traitement pour votre reprise. En suivant les conseils fournis dans le présent document, votre organisation pourra non seulement réduire le temps nécessaire pour se remettre d'une attaque, mais aussi réduire la probabilité d'une attaque ou réduire au minimum les répercussions d'une infection.

Processus de reprise

Comme il a été décrit à la sous-section Élaborer un plan de reprise, le fait de pouvoir compter sur des sauvegardes fiables qui sont sécurisées et stockées hors ligne peut améliorer considérablement votre capacité à vous remettre d'une attaque par rançongiciel. Si votre organisation a été touchée par un rançongiciel, il existe des mesures immédiates que vous pouvez prendre pour réduire au minimum les répercussions d'une infection.

Mesures d'intervention immédiates

Les auteurs de menace peuvent s'infiltrer dans votre réseau afin d'obtenir des renseignements sur les composants et les données de vos systèmes, les dispositifs connectés à votre système et vos communications. Une fois que vous avez connaissance d'une infiltration, vous devez présumer que l'auteur de menace est toujours sur votre réseau et qu'il sait ce qui se passe dans votre organisation. Par conséquent, vous devriez mettre en œuvre une autre méthode de communication (par exemple, un accès aux courriels externes par un dispositif non connecté à votre réseau) à laquelle l'auteur n'a pas accès. Cette méthode permettra également d'empêcher l'auteur de menace de prendre connaissance de vos plans d'intervention en cas d'incident et de vos mesures de reprise. Votre organisation peut suivre la liste de vérification ci-dessous lorsqu'elle prend des mesures de protection immédiates, idéalement dans les premières heures suivant une attaque par rançongiciel.

Liste de vérification pour une intervention immédiate : détection, analyse, endiguement et éradication

Déterminer ce qui est infecté et isoler les systèmes et dispositifs

- Déterminez les dispositifs et les systèmes qui ont été infectés par un rançongiciel.
- Isolez tous les systèmes et dispositifs.

- Déconnectez les systèmes et dispositifs infectés d'Internet et de tout réseau interne pour réduire le risque de propagation de l'infection à d'autres dispositifs connectés.
- Déterminez les données, y compris les données en transit, qui ont été touchées par le rançongiciel.
- Établissez la probabilité que la confidentialité ou l'intégrité des données soient compromises. Avisez les gestionnaires de données et les parties prenantes des répercussions possibles.
- Désactivez vos RPV, serveurs d'accès à distance, ressources à authentification unique ainsi que les biens sur le nuage ou accessibles au public comme mesures supplémentaires pour confiner l'infection par rançongiciel.

Faire un signalement à la police

- Signalez au service de police local toute attaque par rançongiciel. Une attaque par rançongiciel est considérée comme un cybercrime et peut donc faire l'objet d'une enquête policière.
- Signalez également l'attaque par rançongiciel au Centre antifraude du Canada et au Centre pour la cybersécurité en ligne dans Mon cyberportail.
- En cas d'infection par un rançongiciel connu, vérifiez si les forces policières peuvent vous fournir une clé de déchiffrement.

Réunir une équipe d'intervention en cas d'incident

- Transmettez les détails de l'incident à votre équipe d'intervention (équipe mise sur pied lors de l'élaboration de votre plan d'intervention en cas d'incident).
- Donnez des instructions claires aux membres de l'équipe d'intervention quant à leurs rôles et responsabilités dans la gestion de l'incident.
- Prenez en note les détails pour vous assurer que votre équipe d'intervention a bien saisi ce qui s'est produit.
- Répartissez les systèmes touchés par le rançongiciel en vue du rétablissement et de la reprise. Cette mesure aidera votre équipe d'intervention à déterminer où les mesures immédiates à prendre s'imposent.

Changer les justificatifs d'identité

- Réinitialisez les justificatifs d'identité, comme les mots de passe et les phrases de passe, pour les comptes d'administrateur et d'utilisateur.

- Assurez-vous de ne pas changer les justificatifs d'identité nécessaires au rétablissement de votre sauvegarde ou qui pourraient bloquer l'accès aux systèmes dont vous aurez besoin pendant le processus de reprise.
- Créez des comptes d'administrateur temporaires pour commencer votre reprise et déterminez si l'auteur de menace exploite vos comptes initiaux.

Effacer et réinstaller

- Effacez de manière sécurisée le contenu des dispositifs infectés pour enlever les maliciels, les bogues ou les virus.
- Réinstallez le système d'exploitation pour débarrasser vos dispositifs de l'infection.
- Mettez à jour le système d'entrée-sortie de base et rechargez les micrologiciels.

Activer les logiciels de sécurité

- Exécutez les diagnostics antivirus et antimaliciel sur votre sauvegarde pour vous assurer qu'elle n'est pas infectée avant de commencer le processus de rétablissement.
- Rétablissez vos systèmes dans un emplacement propre et isolé du réseau, puis assurez-vous que tous les logiciels sont au niveau de correction le plus récent. Cette action peut prendre du temps et pourrait « rompre » les dépendances au système qui devront être résolues.
- Balayez les fichiers auxquels l'auteur de menace aurait pu avoir accès ou les fichiers qui auraient pu avoir été extraits d'un système compromis.
- Téléchargez Chaîne de montage (Assemblyline), l'outil d'analyse et de détection de maliciels offert gratuitement par le Centre pour la cybersécurité.
- Corrigez tous les éléments signalés par balayage.

Mesures de reprise

L'isolement de votre infrastructure d'Internet peut perturber temporairement vos activités, mais il s'agit de la marche à suivre la plus importante. L'isolement empêchera temporairement l'auteur de menace d'accéder à votre infrastructure, ce qui vous permettra de prendre le contrôle de la situation et d'avancer dans votre processus d'enquête, d'intervention et de reprise.

Lorsque vous aurez franchi les étapes indiquées dans la liste de vérification ci-dessus, et que vous savez sans aucun doute que les sauvegardes et les dispositifs ne présentent aucun maliciel ou virus et qu'ils sont au niveau de correction le plus récent, vous devrez commencer le processus de reprise, comme il est précisé dans les sous-sections suivantes.

Mettre en place des mesures correctives au point d'entrée

Afin d'assurer la réussite de la reprise et d'éviter une nouvelle infection, vous devez découvrir comment l'auteur de menace a réussi à accéder à votre réseau, à vos systèmes et à vos dispositifs, puis corriger la vulnérabilité immédiatement. Assurez-vous de corriger le problème au point d'entrée avant de reconnecter vos systèmes et dispositifs au réseau ou à Internet pour empêcher l'auteur de menace d'y accéder de la même manière.

Mettre en œuvre le plan de sauvegarde

Assurez la protection de votre organisation en ayant en place un plan de sauvegarde détaillé. Vous devez mettre en œuvre ce plan si vos principaux systèmes ainsi que le stockage de vos données ont été compromis et doivent être rétablis à l'aide de la copie de vos données. Grâce au plan de sauvegarde, votre organisation peut rétablir ses données et ses systèmes essentiels, et reprendre ses activités rapidement. La remise en état de vos systèmes devrait se faire au moyen de sauvegardes hors ligne qui ne sont pas connectées à vos réseaux. Avant d'effectuer le rétablissement à partir d'une sauvegarde, balayez et analysez celle-ci au moyen d'un système non corrompu pour vous assurer qu'elle n'a pas été compromise par l'auteur de menace.

Rétablir les systèmes

Conformément à votre plan d'intervention en cas d'incident, déterminez les données et les systèmes essentiels qui doivent d'abord être récupérés. Assurez-vous que ces systèmes et données n'ont pas été touchés par l'attaque par rançongiciel, et qu'ils ne présentent aucun signe d'infection par maliciel.

Plusieurs options sont offertes lors de la mise en œuvre de la stratégie de reprise. Vous devez opter pour une stratégie de reprise qui répond à vos besoins opérationnels et à vos exigences en matière de sécurité.

Faire appel à des professionnelles et professionnels de la cybersécurité

Il peut s'avérer utile de faire appel aux services professionnels d'un organisme de cybersécurité ou d'une ou un professionnel jouissant d'une cote élevée lorsque votre organisation se prépare et intervient en cas d'incident lié à un rançongiciel. Si votre organisation s'est dotée d'une cyberassurance, votre fournisseur offrira souvent l'aide d'un tiers professionnel de la sécurité dans l'éventualité d'un incident, comme une attaque par rançongiciel. Ce professionnel sera en mesure de vous fournir une expertise en matière d'intervention en cas d'incident et une stratégie de reprise adaptée à votre organisation. Il pourrait aussi déployer une équipe de gestion des incidents pour diriger le processus d'intervention et de reprise de votre organisation. Si vous faites appel à de telles personnes, assurez-vous d'établir clairement les attentes, les rôles et les responsabilités liés à leurs services. L'instauration de la cyberassurance comme mesure de protection proactive contre les

rançongiciels peut encourager les entreprises à aligner leurs postures de cybersécurité sur les normes des polices d'assurance. Toutefois, si les documents de police d'assurance ne sont pas adéquatement protégés, des auteurs d'attaques par rançongiciel dotés de moyens sophistiqués pourraient obtenir des renseignements sensibles sur les montants de la couverture et les exploiter lors de négociations de rançon pour maximiser les paiements provenant d'entreprises.

Aviser les parties prenantes

Lorsqu'un incident se produit, et plus particulièrement lorsqu'il compromet vos systèmes et vos données, vous devez absolument aviser les principales parties prenantes, la clientèle et les employées et employés de la situation. Songez à préparer une déclaration qui pourra être adaptée à l'incident, et à dresser une liste comportant les coordonnées de toutes les parties prenantes à aviser. Les attaques par rançongiciel peuvent porter atteinte à la réputation de votre organisation. Il est donc important de mettre en œuvre votre plan de communication rapidement à la suite d'un incident. Vous pourrez alors aviser vos parties prenantes qui, à leur tour, mettront en branle leurs propres plans d'intervention en cas d'incident, le cas échéant.

Analyser l'incident

Il est essentiel de déterminer la cause fondamentale de l'incident. Déterminez comment l'auteur de menace a pu s'introduire dans votre réseau et déployer le rançongiciel. L'incident lié au rançongiciel est souvent un signe de piratage ou d'intrusion plus grave d'un auteur de menace. Si vous n'arrivez pas à déterminer comment s'est produite cette intrusion ou à appliquer les mesures de sécurité appropriées pour éviter qu'elle ne se reproduise, les auteurs de menace pourraient continuer à exploiter la vulnérabilité.

Il convient de noter que, pour réussir en criminalistique, il faut disposer d'un dossier médico-légal de grande intégrité sur les événements. En ce qui concerne les sauvegardes, la surveillance et la journalisation des données doivent faire l'objet d'une séparation rigoureuse des tâches afin de résister à l'attention hostile des auteurs.

Une étape essentielle de l'analyse des incidents consiste à déterminer les systèmes, les comptes et les renseignements auxquels les auteurs de menace ont eu accès. Vous pourrez alors établir l'étendue des dommages en sachant quels comptes ont été compromis et quelles données ont été exfiltrées. Ainsi, vous pourrez mieux contrôler l'attaque, préparer et mettre en œuvre un plan d'intervention approprié, et assurer la réussite de la reprise.

Résumé

Les rançongiciels représentent une menace omniprésente pour toutes les organisations, peu importe leur taille. Les incidents liés aux rançongiciels peuvent faire subir à votre organisation une perte financière, une violation de données et une atteinte à la réputation. Il est important de préparer votre organisation et d'appliquer des mesures proactives pour protéger votre réseau, vos dispositifs connectés et vos renseignements. C'est cette préparation qui vous permettra de réagir à une attaque par rançongiciel et de vous en remettre.

Si votre organisation a été victime d'une attaque par rançongiciel, il est recommandé d'effectuer, après la reprise, un exercice consacré aux leçons tirées. Il s'agit là d'un excellent moyen de mettre en œuvre des mesures d'atténuation complémentaires, et pour corriger les interventions et les stratégies qui n'ont pas donné les résultats escomptés. Révisez votre plan d'intervention en cas d'incident en fonction des leçons tirées pour doter votre organisation des plans d'intervention et de reprise les plus rigoureux qui soient.

Songez à signaler les cyberincidents aux organismes d'application de la loi, comme le service de police local ou le Centre antifraude du Canada, ainsi qu'au Centre pour la cybersécurité en ligne dans Mon cyberportail. Si vous êtes à l'aise de le faire, faites part de vos conclusions au Centre pour la cybersécurité, en indiquant les outils, les techniques et les procédés utilisés par l'auteur de menace. Votre contribution permettra au Centre pour la cybersécurité d'envoyer des alertes et des conseils au public et aidera les particuliers et les organisations à protéger leurs biens contre la même attaque par rançongiciel. La communication des leçons que vous avez tirées pourrait être utile à d'autres organisations et à la collectivité globale de la cybersécurité.

Date d'entrée en vigueur

La présente publication entre en vigueur le 11 décembre 2025.

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour de plus amples renseignements, veuillez communiquer avec le Centre pour la cybersécurité :

- par courriel : contact@cyber.gc.ca;
- par téléphone : 613-949-7048 ou 1-833-CYBER-88.

La présente version du Guide sur les rançongiciels remplace la version antérieure datant du 30 novembre 2021.

Historique des révisions

Révision	Modifications	Date
1	Première version	30 novembre 2021
2	Deuxième version	28 janvier 2026