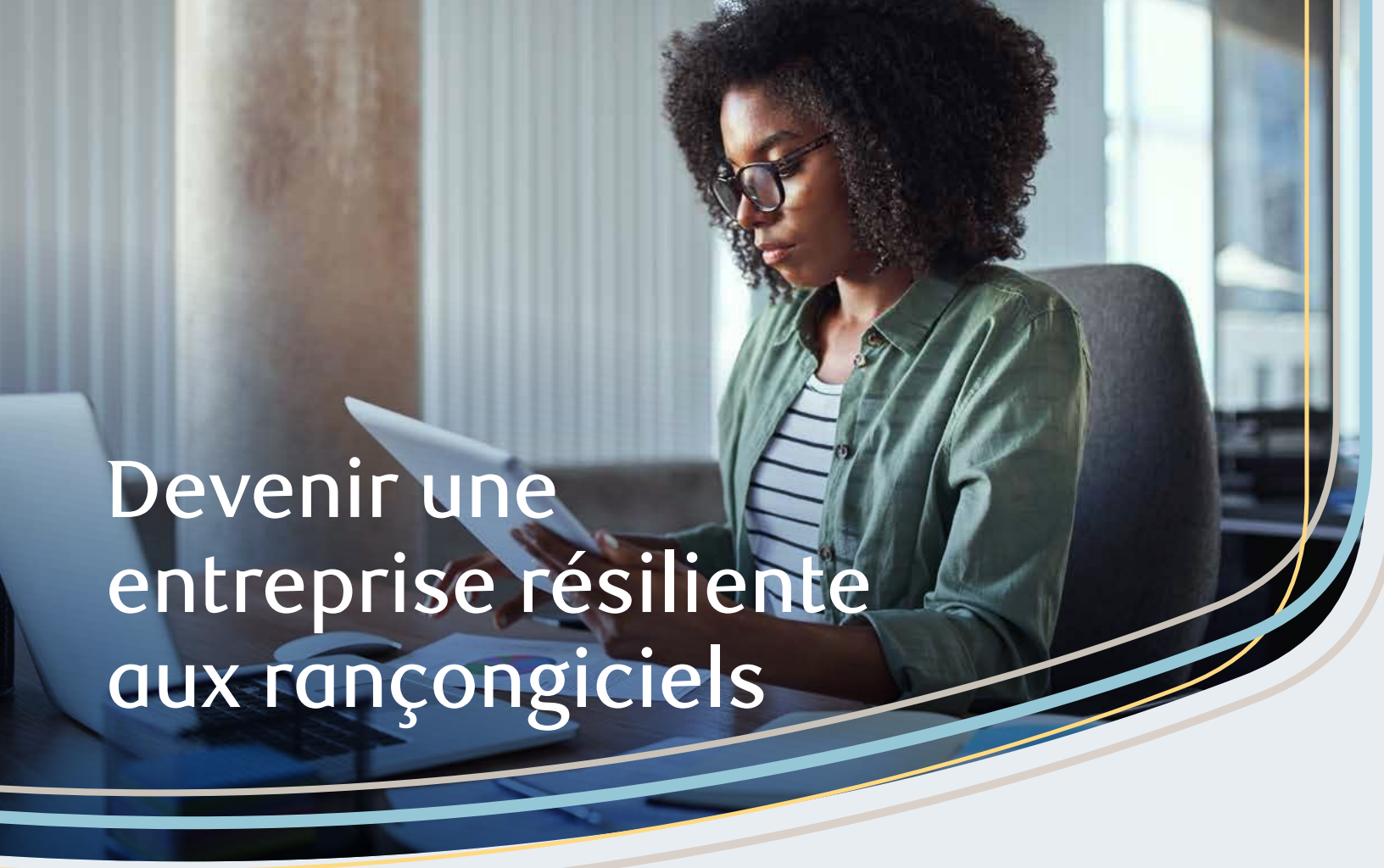


Devenir une entreprise résiliente aux rançongiciels

Sommaire décisionnel: Comprendre les répercussions des maliciels et des rançongiciels sur les entreprises

Les maliciels et les rançongiciels sont actuellement deux des défis les plus préoccupants pour la sécurité des entreprises. Ces types d'attaques sont conçus pour dérober des données sensibles et bloquer l'accès des employés à leurs appareils. Le cybercriminel exige ensuite que l'entreprise paye une rançon en cryptomonnaie pour libérer l'accès au système ou pour restituer les données.

Cela commence souvent fort simplement, mais une attaque peut causer d'importants ravages. Il suffit qu'un seul employé clique sur le mauvais lien ou télécharge une pièce jointe malveillante pour que le maliciel ou le rançongiciel chiffre des données des appareils de votre réseau. Ces attaques peuvent avoir des conséquences majeures sur une entreprise, notamment :

- Interruption de l'activité en raison de la compromission des systèmes
- Coût élevé de la résolution
- Perte de données des clients ou de propriété intellectuelle
- Incapacité à traiter la paie ou à payer les fournisseurs
- Atteinte à la réputation de la marque
- Amendes, poursuites judiciaires et surveillance renforcée des autorités réglementaires

Dans ce document de présentation, nous explorons les répercussions des maliciels et des rançongiciels sur les entreprises. En en comprenant les risques, vous pouvez définir des attentes pour l'ensemble de l'entreprise en matière de conformité et préparer votre équipe informatique pour la réussite.

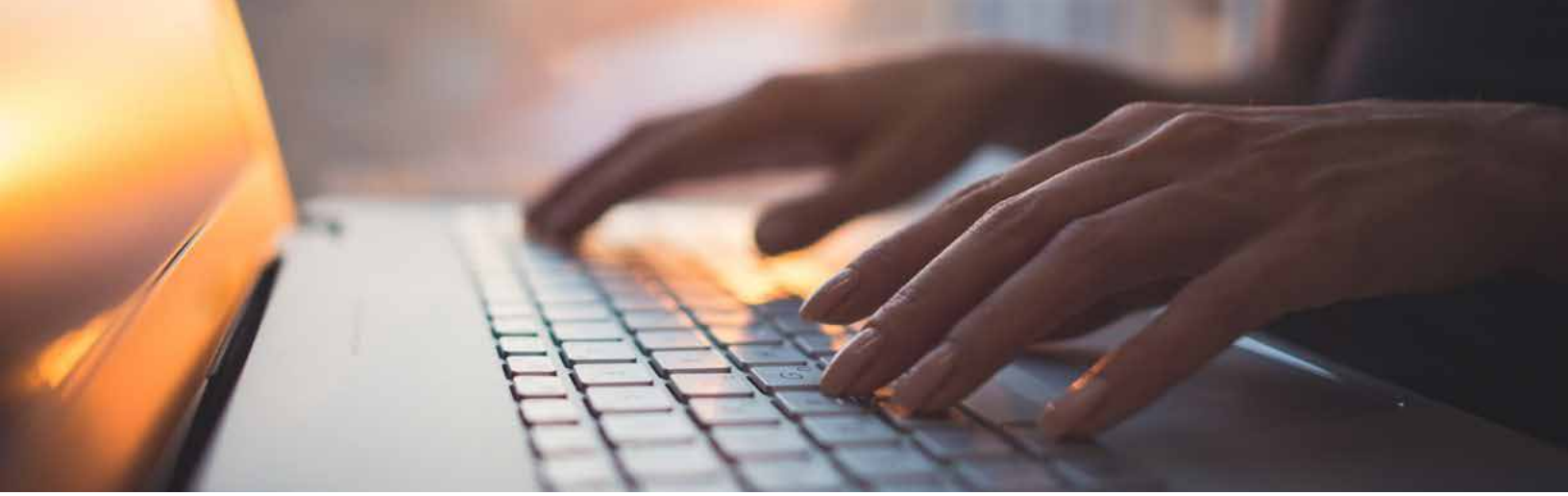
Que pourrait vous coûter une attaque par rançongiciel ?

Coûts associés à des incidents impliquant un rançongiciel aux États-Unis, au Canada et en Europe (USD)

2 730 000 $	Moyenne des demandes de rançon[6]
2 000 000 $	Moyenne des demandes de rançon[6]
5 400 000 $	Moyenne des demandes de rançon pour les grandes entreprises
70 000 000 $	Demande de rançon la plus élevée[8]
40 000 000 $	Rançon la plus élevée payée[12]
1 850 000 $	Moyenne des rançons payées[13]
207 875 $	Moyenne du coût des démarches d'enquête pour les grandes entreprises[15]
40 719 $	Moyenne du coût des démarches d'enquête pour les petites et moyennes entreprises[15]
180 $	Coût d'un dossier perdu ou volé Renseignements identificatoires[10]

Signaler une cyberfraude à RBC.

Si vous pensez avoir été victime d'une attaque par maliciel ou que vos comptes ont été compromis, consultez la page Signaler une fraude à RBC pour obtenir nos coordonnées et communiquer avec nous immédiatement. Notre équipe d'experts peut vous orienter pour prendre les mesures appropriées.



Bienvenue en cyberinsécurité

Qu'elle soit grande ou petite, chaque entreprise s'appuie sur des technologies comme un site de vente en ligne, les courriels, les logiciels infonuagiques et les serveurs pour connecter, collaborer et fonctionner. Toutes ces technologies améliorent l'efficacité, la productivité et l'innovation. Elles augmentent aussi de façon importante le risque de cyberattaque.

Chaque élément de technologie connecté à Internet, depuis les ordinateurs portables, les téléphones intelligents et les tablettes jusqu'aux serveurs, aux capteurs et aux imprimantes, constitue un point d'accès que des cyberpirates peuvent exploiter pour pénétrer dans votre réseau. En 2024, le coût moyen d'un dossier client perdu ou volé s'élevait à 180 $. Pour les PME, le coût moyen d'une violation de données est d'environ trois millions de dollars.[10] Les cyberattaques constituent donc un des défis les plus préoccupants pour les entreprises.

Répercussions organisationnelles des cyberattaques[1]

- Empêcher les employés d'effectuer leur travail quotidien : **33%**
- Atteinte à la réputation de l'entreprise : **28%**
- Frais de résolution ou de récupération payés à des fournisseurs : **27%**
- Perte de revenu : **26%**
- Perte de clients : **26%**
- Nous a dissuadé d'entreprendre les activités prévues : **21%**
- Amende des organismes de réglementation ou des autorités : **18%**
- Paiement de la rançon : **17%**

Signaler une cyberfraude à RBC.

Si vous pensez avoir été victime d'une attaque par maliciel ou que vos comptes ont été compromis, consultez la page Signaler une fraude à RBC pour obtenir nos coordonnées et communiquer avec nous immédiatement. Notre équipe d'experts peut vous orienter pour prendre les mesures appropriées.

État de la situation des cyberattaques

Le nombre d'attaques par rançongiciels a augmenté de 44 pour cent dans le monde en 2024 après que les cyberpirates ont commencé à cibler les entreprises.[2] Non seulement ces attaques sont plus nombreuses, mais elles sont aussi plus coûteuses : à l'échelle mondiale, les pertes de revenu liées à la cybercriminalité atteindront annuellement 10,5 billions de dollars US en 2025, soit une augmentation de 3 billions de dollars US par rapport à 2015.[3]

La lueur d'une bonne nouvelle pointe à l'horizon. En effet, la proportion d'entreprises canadiennes touchées par des incidents de cybersécurité est en baisse : en 2023, environ 16 % des entreprises canadiennes ont été touchées, contre 18 % en 2021 et 21 % en 2019.[10] Cette baisse résulte probablement d'une augmentation des dépenses en prévention et de la formation. En 2024, 55 % des entreprises canadiennes ont rendu la formation à la cybersécurité obligatoire pour tous les employés, contre 32 % en 2019. De plus, les trois quarts des organisations canadiennes ont augmenté leurs ressources financières consacrées à la gestion des systèmes informatiques et à la cybersécurité, et 76 % ont renforcé leurs effectifs dans ces domaines.[4]

Malgré ces baisses, ce n'est pas le moment pour les entreprises de se reposer en criant victoire, car l'intelligence artificielle (IA) permet aux auteurs de menace de mener plus facilement des attaques.

Selon le Sondage 2024 de CIRA sur la cybersécurité, sept répondants sur dix (70 %) s'inquiètent des cybermenaces potentielles que pourrait proférer l'IA générative. Et pour cause : l'autorité réglementaire américaine (Financial Industry Regulatory Authority, FINRA) a souligné l'utilisation croissante de l'IA générative pour créer des courriels d'hameçonnage personnalisés et usurper l'identité d'experts financiers, une tendance confirmée par le FBI.[14] En outre, l'hypertrucage généré par IA – images, sons ou vidéos manipulés – est de plus en plus utilisé pour berner les personnes comme les entreprises.

Les attaques par rançongiciel ont également évolué : les cybercriminels délaissent maintenant les méthodes traditionnelles de chiffrement des données au profit de tactiques d'extorsion directes. Ainsi, les attaquants s'infiltrent dans les systèmes, volent des données sensibles, puis demandent une rançon, menaçant de publier ou de vendre les données si la rançon n'est pas versée. Cette approche élimine la nécessité de chiffrer les données, ce qui permet aux criminels d'exercer une pression par la seule menace d'exposition.

Signaler une cyberfraude à RBC.

Si vous pensez avoir été victime d'une attaque par maliciel ou que vos comptes ont été compromis, consultez la page Signaler une fraude à RBC pour obtenir nos coordonnées et communiquer avec nous immédiatement. Notre équipe d'experts peut vous orienter pour prendre les mesures appropriées.

Comprendre les maliciels et les rançongiciels

Les maliciels et les rançongiciels sont les deux types de cyberattaques les plus courants et nuisibles auxquels une entreprise doit faire face :

Un **maliciel** est un type de programme malveillant conçu pour attaquer et exploiter un appareil. Il en existe différents types, tels que les logiciels espions qui surveillent l'activité d'un appareil, les « bots » (robots) qui utilisent votre appareil pour lancer des attaques et les « rootkits » (maliciel furtif) qui permettent au pirate informatique de prendre le contrôle d'un appareil. Lorsqu'un appareil est compromis par un maliciel, les cyberpirates peuvent l'utiliser pour dérober des données, accéder aux relevés financiers, perturber vos opérations ou comme point d'entrée pour s'en prendre à d'autres parties de votre réseau.

Le **rançongiciel** est un des types de maliciels dont les actualités rendent souvent compte. C'est une attaque qui bloque l'accès à vos données et à vos appareils par chiffrement jusqu'à ce que vous payez une rançon en échange de la clé de chiffrement.

Mode de fonctionnement des rançongiciels

ÉTAPE 1

Le rançongiciel est téléchargé sur un appareil lorsqu'un employé clique sur une pièce jointe. ou un lien malveillant. Un des moyens les plus utilisés pour propager des rançongiciels est le courriel d'hameçonnage qui semble envoyé par une personne fiable et connue de l'utilisateur, telle qu'un collègue ou un client.

ÉTAPE 2

Le rançongiciel se propage dans l'appareil ou sur le réseau à la recherche de données.

ÉTAPE 3

Le rançongiciel chiffre les données, les rendant inaccessibles.

ÉTAPE 4

Le programme fournit les instructions sur la manière de payer la rançon, habituellement en cryptomonnaie que l'on ne peut pas retracer.

ÉTAPE 5

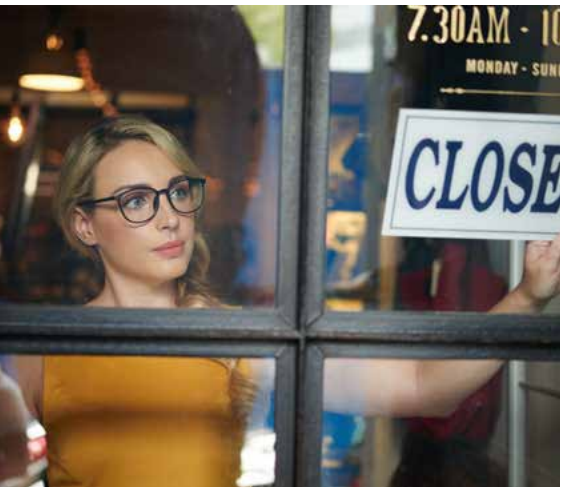
Lorsque la rançon est payée, le programme va supposément fournir une clé de déchiffrement pour permettre à nouveau l'accès.

Signaler une cyberfraude à RBC.

Si vous pensez avoir été victime d'une attaque par maliciel ou que vos comptes ont été compromis, consultez la page Signaler une fraude à RBC pour obtenir nos coordonnées et communiquer avec nous immédiatement. Notre équipe d'experts peut vous orienter pour prendre les mesures appropriées.

Le coût élevé des rançongiciels

L'argent est ce qui motive la plupart des cybercriminels, et les rançongiciels sont donc très utilisés comme méthode d'attaque. Après tout, il est bien plus efficace d'exiger de l'argent que de voler des données pour les vendre ensuite sur le Web profond. Les victimes ont payé environ 1.1 milliard de dollars US de rançon en 2023, soit près du double des 567 millions de dollars payés en 2022.[5] En outre, le versement moyen est passé à deux millions de dollars américains en 2023, soit une augmentation de 500 % par rapport à 2022.[6]



Les coûts liés aux maliciels et aux rançongiciels sont bien plus élevés que l'argent perdu lorsqu'un pirate informatique vide votre compte bancaire ou lorsque vous payez une rançon. Le vol des données de vos clients peut vous exposer à la colère de ceux-ci, à une perte de valeur pour votre marque et à des amendes importantes.

Même une attaque sans perte de données ou d'argent peut perturber le travail des employés et le fonctionnement normal de l'entreprise, et nécessiter beaucoup de temps et d'argent pour enquêter et résoudre le problème. En fait, le coût total de résolution est souvent beaucoup plus élevé que le coût réel de la violation. Par exemple, en juin 2024, un fournisseur de solutions informatiques et de marketing numérique pour l'industrie automobile, a subi une attaque par rançongiciel qui a perturbé les services de milliers de concessionnaires automobiles aux États-Unis et au Canada. Bien que l'entreprise ait payé une rançon de 25 millions de dollars, les concessionnaires touchés ont déclaré des pertes financières combinées d'environ 944 millions de dollars en raison des perturbations opérationnelles au cours des trois premières semaines seulement.[7]

Et pourquoi pas une cyberassurance ? Une cyberassurance pourrait aider à soulager les pertes financières liées à une attaque par rançongiciel, mais elle ne compenserait les autres pertes telles que celles liées à la propriété intellectuelle et l'atteinte à la réputation. En outre, elle ne couvre habituellement pas des choses comme la perte de revenus potentiels ou le coût de mise à jour de vos systèmes à la suite d'une attaque.

Il y a une question à laquelle vous devrez répondre pendant une attaque par rançongiciel : payer ou ne pas payer ? Les experts des autorités chargées de l'application des lois, comme le FBI, recommandent de ne pas payer la rançon, car vous n'avez aucune garantie que le cyberpirate vous redonnera accès aux données.[11] Après avoir payé pour récupérer les données, des cyberpirates cherchent même à extorquer une nouvelle fois de l'argent à leurs victimes en menaçant de divulguer les données volées. Si vous payez, vous pourriez être de nouveau la cible de nouvelles attaques, puisqu'ils savent que vous êtes susceptible de payer à nouveau. De plus, les gouvernements exigent des pénalités civiles et pénales plus importantes pour les entreprises qui payent les rançons afin de décourager le versement de sommes qui financeront ensuite d'autres attaques.

Signaler une cyberfraude à RBC.

Si vous pensez avoir été victime d'une attaque par maliciel ou que vos comptes ont été compromis, consultez la page Signaler une fraude à RBC pour obtenir nos coordonnées et communiquer avec nous immédiatement. Notre équipe d'experts peut vous orienter pour prendre les mesures appropriées.

Comment empêcher les cyberattaques et s'y préparer

L'équipe de l'informatique a la responsabilité d'empêcher les cyberattaques, de détecter et d'y réagir, mais les dirigeants de l'entreprise et tous les employés aussi un rôle à jouer pour assurer la sécurité de l'organisation. Voici quelques-unes des meilleures pratiques que vous pouvez mettre en œuvre immédiatement et avant tout pour empêcher que des maliciels et des rançongiciels aient accès à votre réseau.

Effectuer des sauvegardes conservées hors site.

Établissez une procédure pour sauvegarder toutes les données dans un emplacement sécurisé hors de vos locaux et mettez à jour régulièrement la sauvegarde avec de nouvelles versions des données. Cela vous permettra de rétablir rapidement vos systèmes si vos données sont bloquées par un rançongiciel et vous évitera d'avoir à payer la rançon.

Priorité aux correctifs.

De nombreuses versions de maliciel et rançongiciel exploitent des vulnérabilités connues pour lesquels les fabricants de logiciels ont déjà publié des correctifs. Assurez-vous de mettre en place un processus pour mettre à disposition et installer les mises à jour sur tous les appareils présents sur votre réseau afin de supprimer les failles exploitables connues.

Mettre en œuvre des politiques de sécurité officielles.

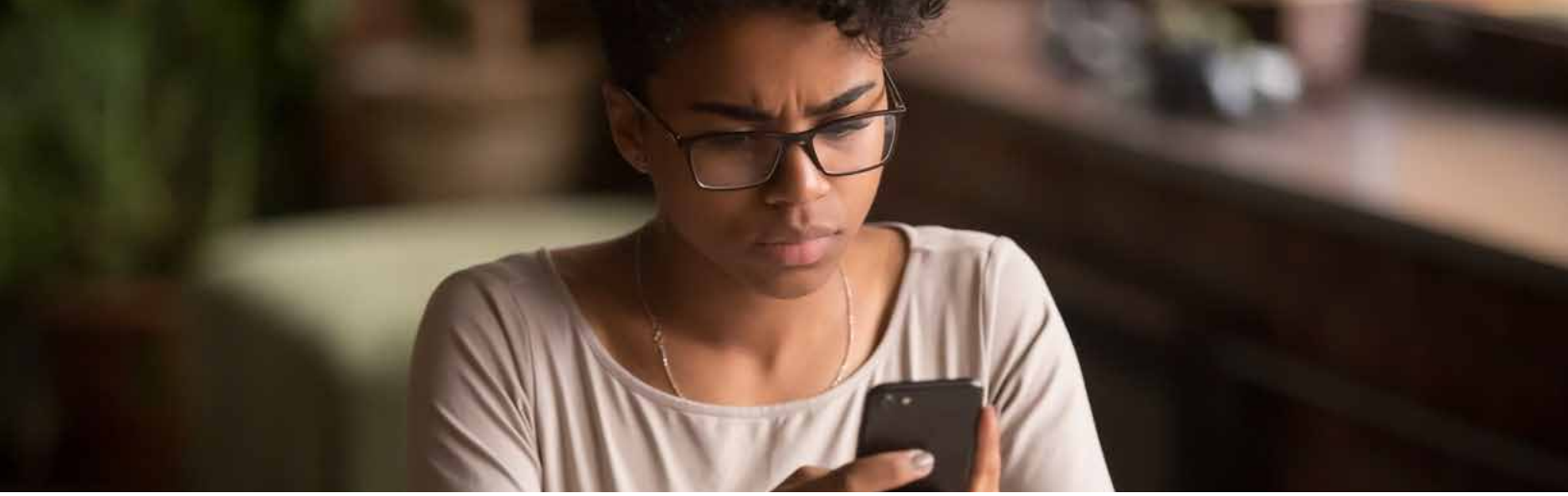
Établissez et faites respecter des politiques de sécurité officielles au sein de votre entreprise pour que les employés n'aient pas à tâtonner en matière de sécurité. Assurez-vous que les employés utilisent des mots de passe complexes et uniques pour s'authentifier dans votre système. Utilisez une authentification multifacteur lorsque c'est possible, et limitez l'accès des employés aux données dont ils ont besoin pour travailler pour qu'un pirate informatique ne puisse pas utiliser leurs identifiants et en prendre le contrôle.

Former les employés.

Il suffit qu'un seul employé télécharge un fichier malveillant et cela coûtera très cher à l'entreprise. Formez les employés aux tactiques d'attaque courantes pour qu'ils sachent comment éviter de télécharger des fichiers dangereux. De plus, assurez-vous qu'ils savent qui appeler au service informatique si leur ordinateur est attaqué. Plus rapidement le service informatique peut mettre un appareil en quarantaine, moins l'attaque est susceptible de se répandre sur le réseau.

Priorité aux investissements dans les technologies de cybersécurité.

Il existe des milliers de produits de cybersécurité qui peuvent réduire les risques liés aux maliciels et aux rançongiciels. Déterminez les points faibles de votre surface d'exposition avec votre équipe du service informatique afin d'investir stratégiquement votre temps, votre argent et vos ressources dans la sécurisation de votre entreprise et la réduction des risques.



Qui devez-vous appeler en cas d'incident ?

Pour beaucoup d'entreprises, la tendance naturelle est de garder le silence concernant une attaque afin d'éviter la publicité. En réalité, 9,6 pour cent des entreprises déclarent les incidents à la police.[9] Cependant, cela vous empêche d'obtenir le soutien dont vous avez besoin pour y répondre efficacement tout en permettant aux criminels de rester libre et de s'attaquer à la prochaine victime mal informée.

Dans la section de votre plan d'intervention en cas d'incident consacrée à la planification et à la préparation, vous devez ajouter les coordonnées de toutes les personnes à informer en cas d'incident. Vous devez communiquer immédiatement avec deux organisations en cas d'attaque :

Les autorités chargées de l'application des lois

Les autorités chargées de l'application des lois locales ou fédérales ont formé des spécialistes qui peuvent vous aider à répondre rapidement. Ils peuvent aussi aider à coordonner vos efforts et à partager les informations avec d'autres agences et services gouvernementaux pour une assistance supplémentaire. Enfin, ils réuniront les preuves essentielles pour mener une enquête criminelle afin que les pirates puissent être traduits en justice.

Les partenaires financiers

Lorsque l'attaque a commencé, il peut être difficile de savoir vers où elle s'oriente et où elle s'arrête. Si vous constatez une activité inhabituelle ou que vous avez déterminé qu'une attaque est en cours, appelez votre banque et vos autres partenaires financiers afin qu'ils puissent surveiller vos comptes et d'éventuelles activités frauduleuses. Les clients RBC doivent consulter la page Signaler une fraude à RBC pour obtenir nos coordonnées et nous appeler immédiatement en cas d'attaque et si un compte est compromis.

Centre canadien pour la cybersécurité

Le Centre canadien pour la cybersécurité travaille avec les autorités chargées de l'application des lois, les entreprises et le secteur public pour diriger la réponse du gouvernement aux événements liés à la cybersécurité.

Courriel : contact@cyber.gc.ca
Numéro sans frais : 1.833.CYBER.88 (1 833 292-3788)

Gardez à l'esprit que les personnes avec qui communiquer diffèrent en fonction des entreprises et des incidents. Appeler la police et la banque peut suffire pour une attaque mineure sur une petite entreprise, mais dans le cas d'une attaque majeure sur un établissement de santé ou une entreprise essentielle, il peut être aussi nécessaire de faire appel à des enquêteurs fédéraux, à des dirigeants élus et à des spécialistes de la cybersécurité.

Même s'ils semblent effroyables, les maliciels et les rançongiciels ne sont qu'une difficulté supplémentaire que vous devez gérer pour votre entreprise. En travaillant avec votre équipe pour mettre en place le plan adéquat, vous pourrez réduire le risque et reprendre vos activités plus rapidement après une attaque.

RBC est à vos côtés pour vous aider à protéger votre entreprise. Visitez rbc.com/cyber/business pour obtenir plus de conseils sur la protection de votre entreprise.

SOURCES

1. CIRA, « perceptions et attitudes des organisations canadiennes à l'égard de la cybersécurité, août 2024».
2. Check Point Software Technologies, « état de la sécurité à l'échelle mondiale en 2025».
3. Cybersecurity Ventures, «Cybercrime to Cost the World $10.5 Trillion Annually by 2025».
4. Pensez cybersécurité, « Où en sont les organisations canadiennes en matière de cybersécurité en 2024 ».
5. Chainalysis, « les versements à des rançongiciels dépassent un milliard de dollars en 2023, un record après une baisse en 2022».
6. Sophos, « L'état des ransomwares 2024 ».
7. Anderson Economic Group, « pertes de 944 millions de dollars au cours des trois premières semaines pour les concessionnaires après la cyberattaque subie par CDK».
8. NetApp, «Comment mesurer le coût réel d'une attaque par ransomwar».
9. Sécurité publique Canada, Profil des entreprises canadiennes qui signalent les cybercrimes à la police.
10. Statistique Canada.
11. FinCEN Guidance, FIN-2020-A00X, « Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, » 1er octobre 2021
12. Business Insider, «L'une des plus grandes compagnies d'assurance américaines aurait payé une rançon de 40 millions de dollars à des pirates informatiques après une cyberattaque.».
13. Astra, « statistiques 2025 sur plus de 100 attaques par rançongiciel : tendances et coûts».
14. The Wall Street Journal, « augmentation du nombre d'escroqueries produites par IA générative selon l'organisme de surveillance de Wall Street».
15. 2021 Palo Alto Networks, Ransomware Threat Report.

Signaler une cyberfraude à RBC.

Si vous pensez avoir été victime d'une attaque par maliciel ou que vos comptes ont été compromis, consultez la page Signaler une fraude à RBC pour obtenir nos coordonnées et communiquer avec nous immédiatement. Notre équipe d'experts peut vous orienter pour prendre les mesures appropriées.