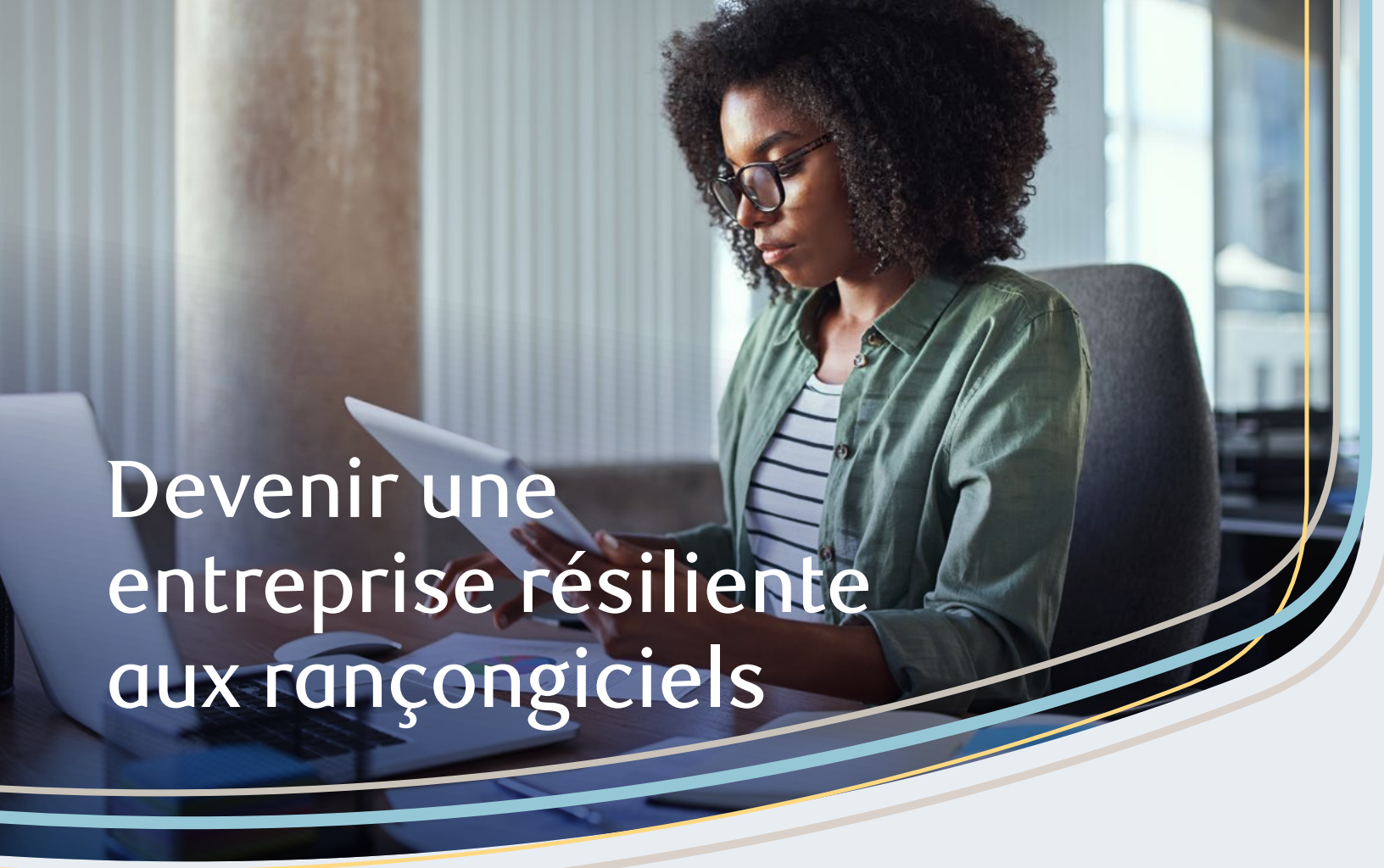


Devenir une entreprise résiliente aux rançongiciels

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.

RBC®

Message de

Lisa Lansdowne-Higgins

Vice-présidente principale, Transformation organisationnelle et dépôts d'entreprise, RBC

Alors que l'adoption des nouvelles technologies par les entreprises continue de s'accélérer, il est essentiel que celles-ci agissent de façon plus proactive pour la sécurisation des données sensibles.

RBC travaille constamment à la modernisation de notre infrastructure pour ouvrir les portes de cette économie numérique à nos clients et à leurs partenaires. Pour cela, nous travaillons avec des partenaires du secteur, des entreprises de technologie financière et des autorités réglementaires.

Alors que le monde poursuit son évolution vers encore plus de services numériques en ligne, les capacités de surveillance en temps réel seront essentielles pour combattre les menaces sur la sécurité informatique. RBC examine régulièrement ses processus de sécurité pour appuyer une analyse en temps réel des virements de fonds grâce à des systèmes de détection de la fraude de calibre international.

Message de

Christina Vandoremalen

Vice-présidente, Dépôts d'entreprise et solutions de trésorerie RBC

Le nombre d'attaques de maliciels et de rançongiciels a augmenté de façon importante et on ne constate aucun ralentissement. Ces attaques représentent un risque majeur pour les clients des Services financiers à l'entreprise (SFE), qu'ils gèrent des petites ou des grandes entreprises.

Pour aider nos clients, RBC cherche en permanence à sensibiliser sur les tendances dans le domaine de la cybersécurité et décrit les moyens de se protéger et de protéger ses activités contre la fraude. Communiquez avec votre conseiller relationnel pour obtenir plus de renseignements sur la façon de protéger votre entreprise.

Si vous êtes un client de RBC et que vous pensez avoir été victime d'une fraude, consultez la page Signaler une fraude à RBC pour obtenir nos coordonnées et communiquer avec nous immédiatement.

Message de

Adam Evans

Vice-président, Cyberopérations et chef de la sécurité de l'information, RBC

Alors que notre monde se numérise de plus en plus, la cybersécurité sera bientôt le principal risque pour les petites entreprises canadiennes. Comme le rapporte le Sondage sur la cybersécurité RBC 2021, près de la moitié des propriétaires d'une petite entreprise au Canada s'attendent à être victimes

d'un cybercrime au cours des 12 prochains mois. Quarante pour cent des petites entreprises déclarent que l'infection d'un appareil de la société par maliciel est maintenant considérée comme une menace plus importante qu'une escroquerie ou une fraude en ligne (24 %) ou des dommages matériels (24 %).

RBC s'engage à vous aider à préserver la sécurité de votre entreprise. Consultez la page Comment protéger votre entreprise pour en savoir plus sur la manière de préparer et protéger votre entreprise contre les incidents de cybersécurité.

* Sondage sur la cybersécurité RBC 2021 réalisé par Ipsos Canada entre le 24 et le 27 août 2021. Plus de 3 000 adultes canadiens ont répondu au sondage en ligne, dans six régions du pays (Colombie-Britannique, Alberta, Saskatchewan/ Manitoba, Ontario, Québec et Canada atlantique).

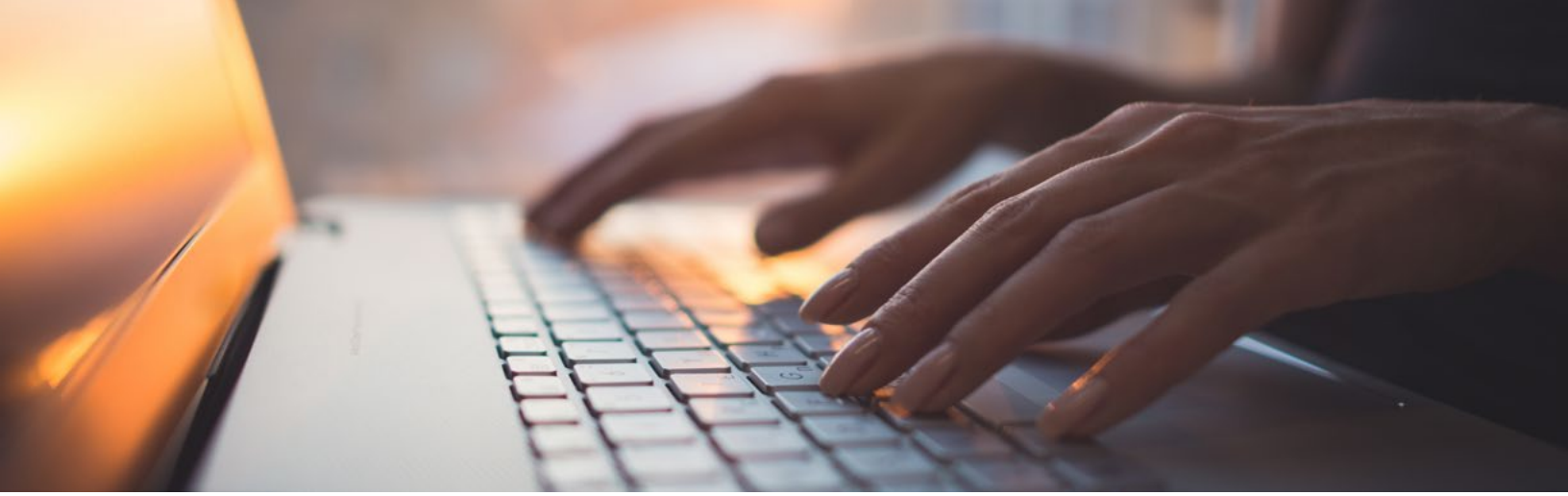
Que pourrait vous coûter une attaque par rançongiciel ?

Coûts associés à des incidents impliquant un rançongiciel aux États-Unis, au Canada et en Europe (USD)[8]

847 344 $	Moyenne des demandes de rançon
718 414 $	Moyenne des demandes de rançon pour les petites et moyennes entreprises
2 923 122 $	Moyenne des demandes de rançon pour les grandes entreprises
30 000 000 $	Demande de rançon la plus élevée
10 000 000 $	Rançon la plus élevée payée
312 493 $	Moyenne des rançons payées
207 875 $	Moyenne du coût des démarches d'enquête pour les grandes entreprises
40 719 $	Moyenne du coût des démarches d'enquête pour les petites et moyennes entreprises
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 2021, le coût moyen d'un dossier client perdu ou volé s'élevait à 180 $, et pour les PME, le coût moyen d'une violation de données était de 2,98 millions de dollars.[10] Les cyberattaques constituent donc un des défis les plus préoccupants pour les entreprises.

Répercussions organisationnelles des cyberattaques[1]

- Restreindre le temps des employés ou empêcher ceux-ci de travailler : **45%**
- Empêcher les employés d'effectuer leur travail quotidien : **33%**
- Frais de résolution ou de récupération payés à des fournisseurs : **19%**
- Atteinte à la réputation de l'entreprise : **19%**
- Perte de revenu : **18%**
- Nous a dissuadé d'entreprendre les activités prévues : **13%**
- Perte de clients : **13%**
- Amende des organismes de réglementation ou des autorités : **9%**
- Paiement de la rançon : **7%**

État de la situation des cyberattaques

Le nombre d'attaques par rançongiciels a augmenté de 435 pour cent dans le monde en 2020 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]

Les cyberattaques constituent un risque pour toutes les entreprises, quelle que soit la taille de celles-ci. Selon l'Enquête canadienne sur la cybersécurité et le cybercrime, au Canada, 18,8 % des petites entreprises, 28 % des moyennes entreprises et 41 % des grandes entreprises ont été la cible d'un incident de cybersécurité ayant eu des conséquences sur leurs opérations.[4]

Et comme dans tous les domaines, la pandémie a rendu la cybersécurité beaucoup plus compliquée. Les employés en télétravail ont souvent accès aux données de l'entreprise par l'intermédiaire de leurs réseaux et appareils personnels non sécurisés, ce qui offre rarement le même niveau de protection que ceux des employeurs situés derrière un pare-feu. Ils peuvent aussi utiliser les appareils fournis par l'entreprise pour un usage personnel et télécharger ainsi des maliciels depuis des sites malveillants qu'ils ne consulteraient pas normalement au bureau. En outre, les employés en télétravail peuvent être distraits par leurs enfants et leur conjoint travaillant ou étudiant dans le même espace, et pourraient donc ne pas porter la même attention nécessaire aux courriels et aux liens.

Résultat : les cyberattaques sont maintenant bien plus menaçantes pour votre entreprise que n'importe quel concurrent. Cela signifie que vous ne pouvez pas demander au service informatique de se soucier seul de la cybersécurité. Les dirigeants d'entreprise responsables de la trésorerie, des finances, des opérations et de la gestion doivent comprendre les risques afin de participer à la prévention des 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.

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

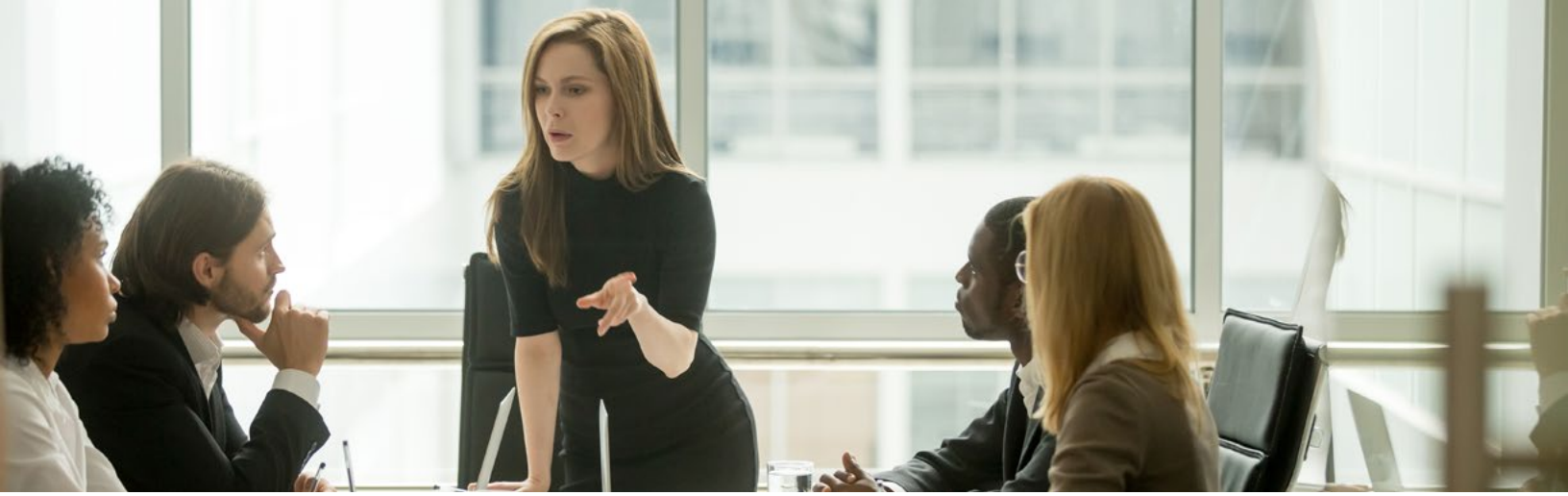
Le programme fournit les instructions sur la manière de payer la rançon, habituellement en cryptomonnaie que l'on ne peut pas retracer.

ÉTAPE 5

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

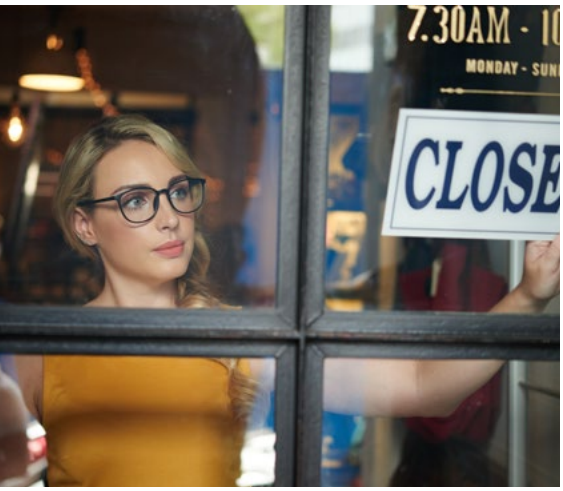
Signaler une cyberfraude à RBC.

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 350 millions de dollars US de rançon en 2020, soit une augmentation de 311 % par rapport à l'année précédente.[5] De plus, les rançons s'élevaient en moyenne à 312 493 $ US en 2020, en augmentation de 171 % par rapport à 2019.[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, la ville d'Atlanta a subi une attaque par rançongiciel pour laquelle une rançon de 50 000 $ US était exigée. Mais le total des coûts de résolution a dépassé 2,6 millions de $ US en raison des dépenses liées à la réponse à l'incident, aux enquêtes numériques, au personnel supplémentaire nécessaire et à la communication de crise.[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 du service informatique a la responsabilité d'empêcher et de détecter les attaques, et d'y répondre, mais les dirigeants de l'entreprise et tous les employés ont un rôle à jouer pour préserver la sécurité. 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.

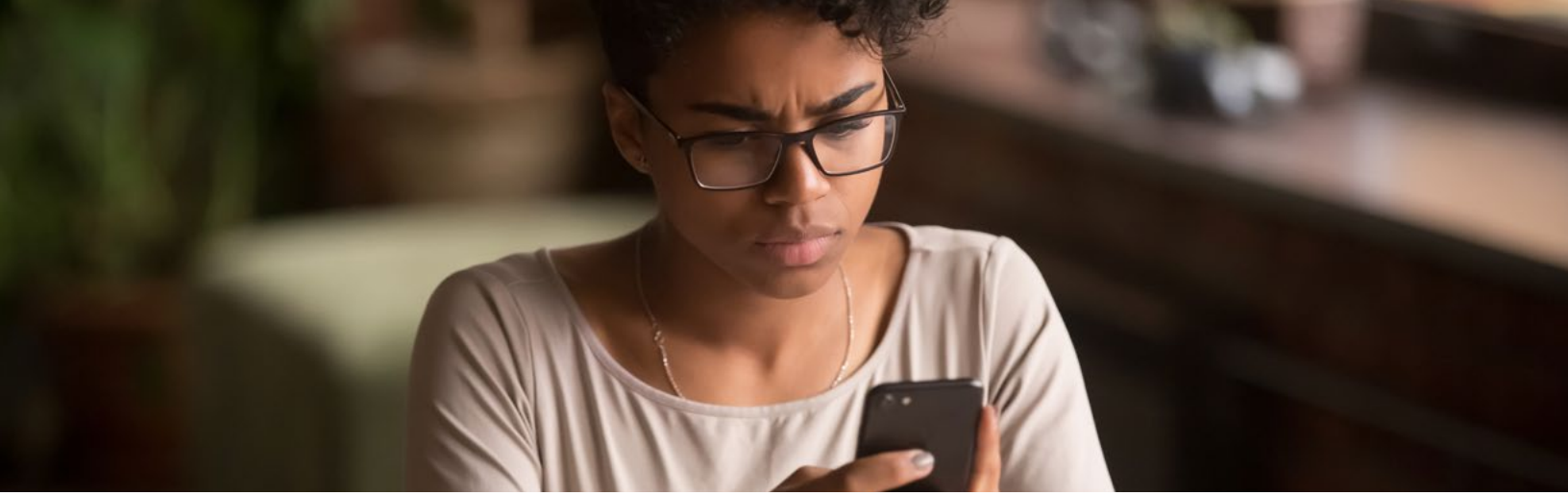
Établissez et faites respecter des politiques de sécurité officielles au sein de votre entreprise pour que les employés n'aient pas à tâtonner en matière de sécurité. Assurez-vous que les employés utilisent des mots de passe complexes et uniques pour s'authentifier dans votre système. Utilisez une authentification 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

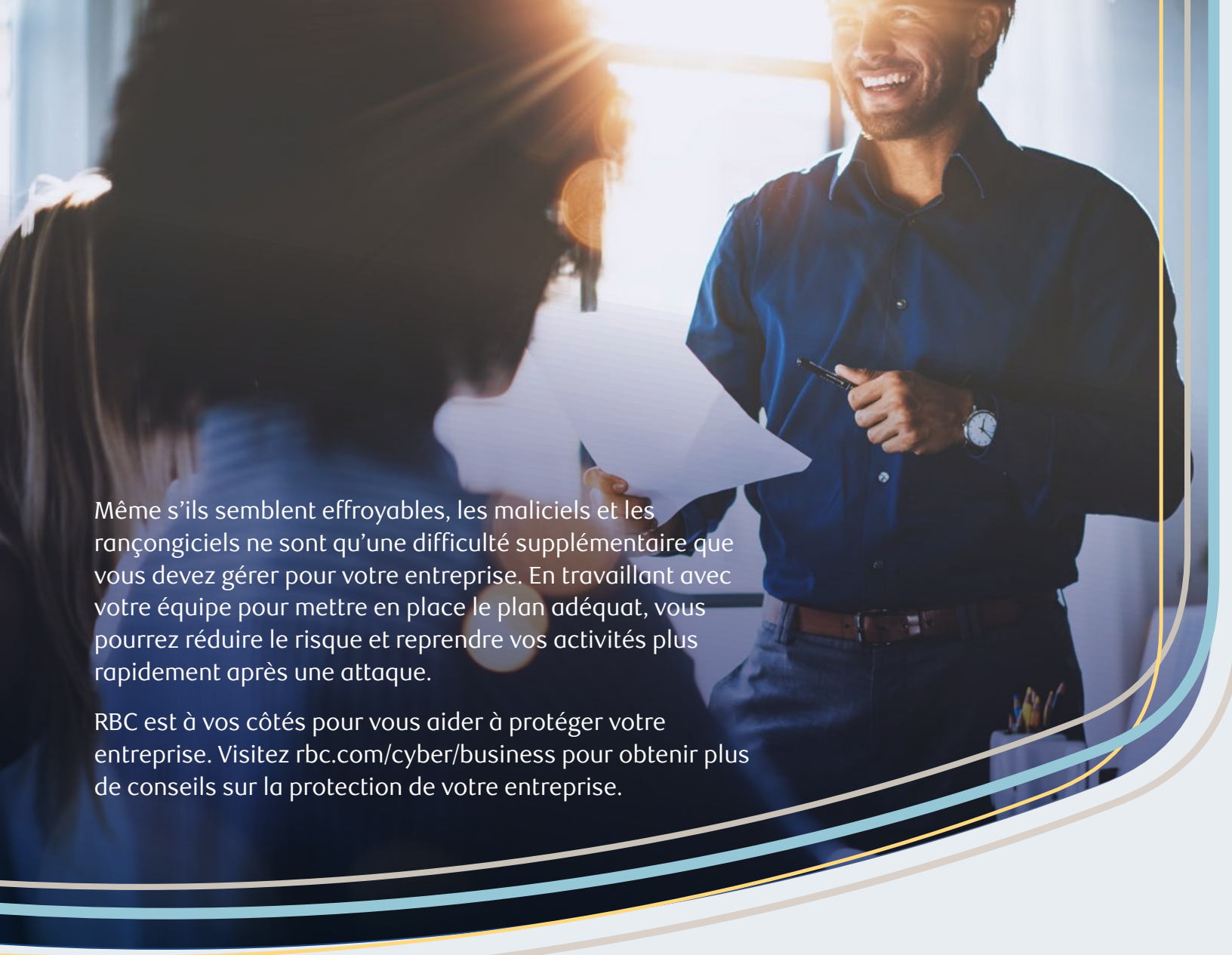
Lorsque l'attaque a commencé, il peut être difficile de savoir vers où elle s'oriente et où elle s'arrête. Si vous constatez une activité inhabituelle ou que vous avez déterminé qu'une attaque est en cours, appelez votre banque et vos autres partenaires financiers afin qu'ils puissent surveiller vos 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. Sondage de CIRA sur la cybersécurité, 2021.
2. Deep Instinct, Ransomware: Prevention is Better than the Cure.
3. Cybersecurity Ventures, Cybercrime to Cost the World $10.5 Trillion Annually by 2025.
4. Sécurité publique Canada, Profil des entreprises canadiennes qui signalent les cybercrimes à la police.
5. Chainalysis Team, Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think.
6. Palo Alto Networks, Ransomware Threat Report.
7. Wired, Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Attack.
8. 2021 Palo Alto Networks, Ransomware Threat Report.
9. Sécurité publique Canada, Profil des entreprises canadiennes qui signalent les cybercrimes à la police.
10. IBM Security, Cost of a Data Breach Report 2021
11. FinCEN Guidance, FIN-2020-A00X, « Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, » 1er octobre 2021

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.