PARLONS
PRÉVENTION

ATTAQUES PAR RANÇONGICIEL : CONTEXTE ACTUEL DES MENACES

Les entreprises canadiennes font face à des menaces à tactiques d'extorsion multiple

Les attaques par rançongiciel sont la cybermenace la plus courante pour les entreprises canadiennes, et les extorsions multiples sont devenues la norme. Les cyberpirates emploient maintenant divers moyens pour exercer un maximum de pression : cryptage de données, vol de renseignements de nature délicate, menaces de divulgation d'information ou de surveillance réglementaire, etc. Voici un résumé des tendances actuelles et des mesures pratiques que les entreprises peuvent prendre.

Northbridge[MD]
Assurance

LES EXTORSIONS MUTIPLES : DÉSORMAIS LA NORME

Les tactiques d'attaque par rançongiciel ont changé. De nos jours, en plus de viser à perturber les systèmes, elles peuvent inclure la copie de données de nature délicate et des menaces de divulgation et de surveillance réglementaire. Selon le Centre canadien pour la cybersécurité (CCC), les attaques par rançongiciel sont **la cybermenace la plus courante au pays**, et leur fréquence ainsi que leur incidence continuent d'augmenter.

Pourquoi est-ce important?

Les entreprises peuvent être vulnérables au vol et aux fuites de données même si elles ont de bonnes stratégies de sauvegarde. En cas d'incident, les conséquences peuvent être multiples : signalement de la situation aux autorités réglementaires, dépenses supplémentaires en lien avec la confidentialité des données, interruptions inattendues, atteinte à la réputation, etc.

Selon le CCC, le nombre d'attaques par rançongiciel signalées a augmenté de **26 %** par année en moyenne depuis 2021, ce qui confirme qu'elles continuent de prendre de l'ampleur et d'évoluer au Canada[1].

Pourquoi les entreprises canadiennes sont-elles vulnérables?

- Atteintes par l'intermédiaire de la chaîne d'approvisionnement : À l'heure actuelle, plutôt que de cibler directement les systèmes des entreprises, les cyberpirates y accèdent souvent par l'intermédiaire d'un fournisseur de confiance. Donc les risques auxquels une entreprise est exposée ne dépendent pas uniquement des mesures de contrôle qu'elle prend, mais aussi de celles que ses partenaires prennent.
- Divers secteurs dans la mire des cyberpirates : De nombreux secteurs ont eu à faire face à des interruptions et à de coûteuses reprises de leurs activités au cours des dernières années, notamment les secteurs du transport et de la logistique, des soins de santé (cliniques, établissements de soins de longue durée, fournisseurs de soins auxiliaires), des technologies, des services publics et de la fabrication. Le CCC estime que **la tendance se maintiendra pour les entreprises et les infrastructures essentielles de toutes tailles**.
- Manque de préparation des petites entreprises : **47 %** des petites entreprises affirment se sentir plus préoccupées par les attaques par rançongiciel qu'avant la pandémie, mais seulement **24 %** disent avoir souscrit une cyberassurance. Elles ne semblent donc pas être suffisamment préparées à faire face aux incidents[2].
- Sous-estimation des coûts réels : Le CCC croit que la majorité des attaques par rançongiciel au pays pourraient ne pas être signalées aux autorités, ce qui signifie que le volume d'incidents et les coûts perçus par le public sont probablement inférieurs à la réalité[3].

FAIBLESSES SOUVENT EXPLOITÉES

Accès initial : Pour entrer dans les systèmes, les cyberpirates peuvent se servir de courriels d'hameçonnage, utiliser des identifiants de connexion volés ou réutilisés, ou exploiter des systèmes externes qui ne sont pas à jour. Des employés peuvent ouvrir des courriels bien convaincants. Des accès publics peuvent aussi rendre les systèmes vulnérables.

PENSEZ-Y...

Si un jeu de données sur vos clients se retrouvait en ligne demain matin, comment expliqueriez vous la situation à ces derniers et aux autorités réglementaires? Que feriez-vous pour que les données soient retirées? Auriez-vous l'obligation d'informer vos clients de l'incident?

Propagation interne : De nombreuses entreprises se concentrent sur la protection du périmètre de leur réseau et présument que leurs systèmes internes sont bien sécurisés. Mais une fois le périmètre de défense percé, les cyberpirates peuvent naviguer dans le réseau interne, surtout lorsque les droits d'accès des comptes utilisateurs sont plus étendus que nécessaire et que les systèmes ne sont pas bien isolés les uns des autres. Un simple incident peut alors dégénérer rapidement et causer de graves dommages.

Compromission des sauvegardes : Si les cyberpirates trouvent les sauvegardes sur le même réseau que les systèmes visés, ils s'y attaquent souvent en premier pour les désactiver et les chiffrer. Un incident récupérable au départ peut ainsi se transformer en une perturbation beaucoup plus sérieuse.

Exfiltration et extorsion : Dans bien des cas, les cyberpirates exploitent, pour leurs vols et leurs extorsions, les systèmes qui ont le plus de droits d'accès, comme les postes d'administrateurs. Ils peuvent aussi cibler les failles dans la protection évolutive des points de terminaison (PEPT) et dans les contrôles de prévention de la perte de données (DLP) pour voler et extraire des données sensibles sans se faire repérer.

MESURES PRATIQUES

Voici quelques conseils pour vous aider à établir vos priorités concernant les mesures de sécurité.

Contrôles des accès

- **Authentification multifacteur (AMF) forte :** Activez l'AMF pour les courriels, l'accès à distance au réseau privé virtuel (RPV) et tous les comptes bénéficiant de nombreux droits d'accès ou d'autres privilèges. Bien qu'aucune mesure de contrôle ne soit infaillible, l'AMF réduit considérablement le risque que des cyberpirates accèdent à vos systèmes en utilisant des identifiants volés.
- **Droit d'accès minimal :** Ne donnez aux employés et aux utilisateurs externes que les accès dont ils ont réellement besoin pour effectuer leur travail. Ainsi, vous réduirez le rayon d'action des cyberpirates si jamais ils réussissent à entrer dans vos systèmes.

Résilience

- **Sauvegardes fiables :** Conservez des sauvegardes dans différents environnements. Ayez, notamment des sauvegardes en lecture seule (ou protégées en écriture) et des répliques hors ligne pour assurer une certaine redondance et faciliter la récupération en cas de besoin. Souvent appelées « sauvegardes immuables », ces sauvegardes ne peuvent pas être supprimées ni altérées, que ce soit par des cyberpirates informatiques ou de façon accidentelle. Des tests réguliers des sauvegardes redondantes favorisent aussi une reprise rapide et fiable après un incident.

- **Établissement de vos fournisseurs essentiels :** Assurez-vous d'avoir au moins une copie de sauvegarde pour chacun de ces fournisseurs, et tenez à jour un registre commun simple (indiquant les délais de livraison, les tarifs et les responsables des commandes) pour réduire les risques que vos activités soient perturbées. Cela vous évitera de recourir à des outils complexes ou d'investir des sommes importantes.
- **Application rapide de correctifs aux systèmes connectés à Internet :** La première chose que les cyberpirates font est souvent d'exploiter les vulnérabilités connues des systèmes connectés à Internet. Donc, dès que des correctifs sont disponibles, appliquez-les en priorité à vos systèmes vulnérables.

Facteurs humains

- **Les employés comme première ligne de défense :** De nombreuses attaques par rançongiciel commencent par un courriel d'hameçonnage convaincant. Pour aider les employés à reconnaître les messages suspects et vous permettre de faire un suivi des progrès au fil du temps, offrez-leur régulièrement de courtes formations de sensibilisation et faites périodiquement des simulations d'hameçonnage. De plus, assurez-vous de redoubler de prudence, car les cyberpirates se tournent de plus en plus vers l'intelligence artificielle (IA) pour produire des courriels d'hameçonnage de masse plus réalistes que jamais.

Capacité de réponse

- **Définition et mise à l'essai d'un plan d'intervention :** Élaborez un plan d'intervention qui établit clairement les rôles et les responsabilités au cours des premières heures suivant une attaque. Demandez-vous régulièrement ce qu'il se passerait si vous étiez victime d'une attaque par rançongiciel aujourd'hui. Faites des simulations avec différentes équipes — TI, Communications, Service juridique et responsables de la protection des données — pour vous assurer que chacun comprend son rôle et pourra réagir rapidement et efficacement en cas de besoin.

Moyens simples d'évaluer votre préparation

- **Restauration à partir de sauvegardes :** Avez-vous réussi à restaurer un système essentiel à partir d'une sauvegarde sécurisée au cours des 90 derniers jours?
- **Utilisation de l'AMF :** Avez-vous activé l'AMF pour les courriels, l'accès à distance et les comptes qui disposent de nombreux privilèges d'accès?
- **Vitesse d'application des correctifs :** Dans les systèmes connectés à Internet, à quelle vitesse les vulnérabilités importantes sont-elles corrigées?
- **Préparation en cas d'incident :** Si vous ne disposez pas encore d'un plan d'intervention en cas d'incident, c'est le moment d'en élaborer un. Si vous en avez déjà un, avez-vous fait des simulations pour le tester?

ASSURANCE DES CYBERRISQUES OFFERTE PAR NORTHBRIDGE ASSURANCE

Votre filet de sécurité

Même des mesures de contrôle rigoureuses ne peuvent éliminer entièrement les risques. Mais transférer vos risques peut vous fournir un filet de sécurité. Northbridge propose **une solution complète pour contribuer à couvrir les cyberrisques** (de l'assuré et des tiers), incluant une protection Vol lié aux cyberrisques en option. Elle offre également **les services Assistance Cyberrisques** (analyse des vulnérabilités, autoévaluation, simulations d'incidents) aux clients admissibles afin de soutenir les programmes de gestion des risques.

Pour savoir comment mieux protéger votre entreprise, communiquez avec le Service de prévention au **1.833.692.4111** ou rendez-vous sur notre site **www.northbridgeassurance.ca**.

PENSEZ-Y...

Si les systèmes de courriel et de partage de fichiers ne fonctionnaient pas pendant 3 jours, quelles équipes en souffriraient le plus et quelle solution manuelle appliqueriez-vous?

[1] *Vue d'ensemble des menaces par rançongiciel de 2025 à 2027*, Centre canadien pour la cybersécurité, 2025.
[2] Sondage Léger sur la cybersécurité des petites entreprises commandé par le BAC, 2021.
[3] *Guide sur les rançongiciels*, Centre canadien pour la cybersécurité, 2026.