LE CENTRE CANADIEN POUR LA CYBERSÉCURITÉ PUBLIE UN GUIDE SUR LES RANÇONGICIELS

Publié le 29 décembre, 2021

Catégories: Perspectives, Publications

Les attaques par rançongiciel sont de plus en plus fréquentes.

Dans le monde, elles ont connu une hausse effarante de 151 % à la première moitié de 2021[1]. Et de nombreuses grandes organisations ont été prises pour cible – il suffit de penser à Kaseya ou à Colonial Pipeline, qui ont fait les manchettes cet été.

Le Centre canadien pour la cybersécurité (le « **CCC** ») propose plusieurs pistes pour expliquer cette augmentation de la fréquence des attaques par rançongiciel, dont l'adoption de méthodes de travail en ligne en raison de la pandémie et la sophistication accrue des techniques de cybercriminalité[2].D'ailleurs, on constate l'émergence troublante d'un modèle d'affaires « rançongiciel-service » : des développeurs vendent ou louent leurs programmes à d'autres cybercriminels en échange d'une partie du magot[3].

Néanmoins, le CCC souligne que la vaste majorité des attaques par rançongiciel peuvent être parées par des mesures de cybersécurité élémentaires. C'est dans ce contexte qu'il a publié le 30 novembre un guide sur les rançongiciels (le « **guide** ») pour aider les organisations à préparer leurs plans de défense et d'intervention[4].

Qu'est-ce qu'un rançongiciel?

Les rançongiciels sont des logiciels malveillants qui menacent de publier les données de la victime ou de bloquer l'accès à un système à moins qu'une rançon ne soit payée. Ils interrompent des fonctionnalités critiques dépendant d'une connexion réseau ou système, ce qui peut entraîner des conséquences dévastatrices.

Quels types d'entreprises sont ciblés?

Les entreprises de toutes tailles peuvent être victimes d'un rançongiciel. Le guide indique que si les attaques sur les grandes entreprises sont peut-être plus lucratives, souvent, les cybercriminels estiment que les PME ont des mesures de sécurité moins efficaces, ce qui en fait des cibles faciles[5].

Voici quelques facteurs qui augmentent les risques d'être visé :

- L'entreprise a accès à des données sensibles qui peuvent être exploitées directement (p. ex., NAS, numéros de carte de crédit, renseignements financiers);
- L'entreprise a accès à des renseignements confidentiels (p. ex., de nature médicale ou religieuse);
- Les données sont essentielles au fonctionnement de l'entreprise, et une interruption des systèmes stopperait toute activité (et inciterait l'entreprise à payer la rançon);
- L'entreprise détient de précieuses données sur ses clients ou des données de propriété intellectuelle (p. ex., secrets commerciaux);
- L'entreprise offre des services essentiels (p. ex., services médicaux critiques);
- L'entreprise fait affaire avec une entreprise qui remplit l'un des critères qui précèdent[6].

La première moitié du guide porte sur les moyens de défense contre les rançongiciels. Elle traite de la planification de la cybersécurité et des contrôles de base. On y trouve les principes qui sous-tendent la création d'un plan de sauvegarde, d'un plan d'intervention en cas d'incident et d'un plan de reprise[7], de même qu'une liste de mesures de sécurité pertinentes, dont :

- **Les défenses de périmètre**, comme les pare-feu, les logiciels antihameçonnage et les réseaux privés virtuels;
- **La journalisation et les alertes**, pour surveiller l'activité dans l'ensemble du système et établir une piste de vérification.
- **Les tests de pénétration**, pour évaluer les vulnérabilités;
- **La segmentation réseau**, pour contrôler et restreindre l'accès aux données du réseau informatique;
- **La gestion des mots de passe**, pour assurer la robustesse des mots de passe utilisés[8].

La deuxième moitié du guide porte sur ce qu'il faut faire en cas d'attaque. Elle traite des mesures à prendre immédiatement lorsque l'attaque survient et des gestes qui peuvent aider à reprendre les activités aussi rapidement que possible[9].

Le guide aidera les entreprises de toutes tailles à évaluer leur niveau de préparation face aux rançongiciels et, au besoin, à l'améliorer. Cependant, la sécurité des données nécessite une approche contextuelle, c'est-à-dire qu'il faut tenir compte de la nature des activités, des données et des systèmes de sécurité. Pour établir une stratégie de rançongiciels exhaustive, il faut avoir recours à des professionnels du droit et des TI.

Si vous avez été victime d'un rançongiciel ou que vous vous demandez quoi faire pour parer cette menace, communiquez avec un membre de notre groupe Protection de la vie privée et des données.

[1][ps2id id='1' target=''/] En comparaison avec la 2e moitié de 2020 : Centre canadien pour la cybersécurité, *Bulletin sur les cybermenaces : La menace des rançongiciels en 2021*.

[2][ps2id id='2' target='/]Centre canadien pour la cybersécurité, *Bulletin sur les cybermenaces : La menace des rançongiciels en 2021*, « Tendance en cours d'évolution ».
[3][ps2id id='3' target='/]Centre canadien pour la cybersécurité, Bulletin sur les cybermenaces : La menace des rançongiciels en 2021, « Rançongiciel comme service ».
[4] [ps2id id='4' target='/] Centre canadien pour la cybersécurité, Guide sur les rançongiciels ITSM.00.099.
[5][ps2id id='5' target='/] Centre canadien pour la cybersécurité, Guide sur les rançongiciels ITSM.0.099, section 1.1.2.
[6][ps2id id='6' target='/] Centre canadien pour la cybersécurité, Guide sur les rançongiciels ITSM.0.099, section 1.1.2.
[7][ps2id id='7' target='/] Centre canadien pour la cybersécurité, Guide sur les rançongiciels ITSM.0.099, section 2.1.
[8][ps2id id='8' target='/] Centre canadien pour la cybersécurité, Guide sur les rançongiciels ITSM.0.099, section 2.2.
[9][ps2id id='9' target='/] Centre canadien pour la cybersécurité, Guide sur les rançongiciels ITSM.0.099, section 3.

par Mitch Koczerginski et Robbie Grant

Mise en garde