Alliance for Healthier Communities
Alliance pour des communautés en santé

Cybersécurité et rançongiciels

Membres d'Alliance – Étude de cas

Table des matières

« Les rançongiciels sont un cybercrime particulier, puisque **pour que l'attaque** réussisse, la victime doit être complice après le fait »

– James Scott[1]

Vous êtes une victime du rançongiciel PETYA!
Les disques durs de votre ordinateur ont été chiffrés au moyen d'un algorithme de chiffrement de niveau militaire. Il est impossible de restaurer vos données sans utiliser une clé spéciale. Vous pouvez acheter cette clé aux adresses mentionnées au point 2 ci-dessous se trouvant dans le Darknet.

Veuillez suivre les trois étapes faciles suivantes pour acheter votre clé et restaurer vos données :

1. Téléchargez le navigateur Tor que vous trouverez à l'adresse https://www.troproject.org/. Si vous avez besoin d'aide, faites une recherche des mots clés « access onion page » sur Google.
2. Visitez l'une des pages suivantes en utilisant le navigateur Tor :

http://petya37h5tbhyvki.onion/N19fvE
http://petya37h5tbhyvki.onion/N19fvE

3. Inscrire votre code de décryptage personnel ici :

Si vous avez déjà acheté votre clé, veuillez l'inscrire ci-dessous :

Clé :

[1] Auteur de l'ouvrage intitulé *The CEO's Manual on Cyber Security*

Introduction

Les rançongiciels sont un type de programme ou logiciel malveillant qui verrouille tous les fichiers connus au moyen d'un chiffrage puissant, ce qui empêche les utilisateurs et administrateurs d'accéder à leurs réseaux, systèmes et données. Les rançongiciels empêchent efficacement l'accès aux données de l'organisme au moyen du chiffrement, puis le refus de fournir les outils de décryptage à moins qu'une rançon soit payée. Or, lorsque nous payons la rançon, nous présumons que les pirates ont un sens de l'éthique. Dans les faits, il n'existe aucune garantie que ce paiement assurera l'obtention de la clé de décryptage requise pour accéder aux données. L'unique objectif des rançongiciels est de faire en sorte que les gens ne puissent pas accéder à leurs fichiers électroniques.

Cyberattaques par rançongiciel

Les pirates qui utilisent les rançongiciels demandent habituellement un paiement en cybermonnaie (p. ex. en bitcoin), car ces moyens de paiement sont très difficiles à retracer. Les rançongiciels peuvent infecter les réseaux et les ordinateurs de plusieurs façons. Une des façons les plus courantes est au moyen de pourriels malveillants ou de courriels non sollicités par lesquels sont envoyés les programmes malveillants. Ces types de courriels peuvent contenir des pièces jointes empoisonnées telles que des PDF ou des documents Word qui semblent légitimes. Ils peuvent également contenir des liens qui semblent inoffensifs vers des sites Web malveillants. Ces méthodes, qui sont fondées sur le piratage psychologique, trompent les gens en leur faisant croire que les pièces jointes ou les liens sont légitimes pour que ces derniers ouvrent les pièces ou cliquent sur les liens. Les messages courriel semblent provenir d'amis de collègues ou d'institutions de confiance.

Une autre façon courante est l'attaque par force brute[2]. Cette méthode consiste à tenter d'obtenir le mot de passe ou le NIP de l'utilisateur au moyen d'essais et d'erreurs. Des logiciels automatisés sont utilisés pour générer un grand nombre de possibilités d'un mot de passe. Ces types d'attaques sont l'une des raisons pour lesquelles on vous demande souvent de « prouver que vous n'êtes pas un robot » lors de la création ou de l'inscription d'un mot de passe d'un compte.

Les établissements de soins de santé visés

Les établissements de soins de santé sont devenus des cibles faciles pour les pirates, puisque ces établissements utilisent des dossiers médicaux électroniques contenant des données et des renseignements sensibles sur l'organisme. Ces dossiers contiennent aussi habituellement l'ensemble des données requises permettant aux pirates de voler des identités, de frauder les compagnies d'assurance, de chiffrer les données pour obtenir des rançons, de consulter les données à la recherche de renseignements et de voler la propriété intellectuelle. Cependant, la principale raison pour laquelle les pirates visent les établissements de soins de santé est le manque de financement à l'échelle du pays pour l'acquisition de systèmes de TI qui assureraient la cybersécurité.[3].

[2] Pour en savoir plus sur les attaques par force brute, veuillez consulter la page https://www.techopedia.com/definition/18091/brute-force-attack

[3] https://www.cbc.ca/news/canada/new-brunswick/david-shipley-medical-devices-cybersecurity-1.4236458

Les rançongiciels sont devenus plus sophistiqués et les recettes potentielles provenant de ces activités criminelles ont augmenté. De nos jours, ce type de programme malveillant est plus dissimulé et infecte en catimini, ce qui permet aux pirates informatiques de voler des données tout en les chiffrant localement. Même si vous obtenez une clé de décryptage, si une analyse de l'événement montre que le programme malveillant permet d'envoyer une copie de vos données à un autre emplacement hors site, le potentiel de faire l'objet d'attaques pour rançons et d'atteinte aux lois relatives à la protection de la vie privée et à la sécurité pourrait augmenter. Les études de cas suivantes, qui portent sur des cyberattaques qui ont eu lieu dans quatre organismes membres différents, exposent la raison précise pour laquelle ces organismes ont été visés par cette cyberattaque

Étude de cas nº 1

Détails de la cyberattaque

La cyberattaque en question est survenue au courant de la fin de semaine. Tous les ordinateurs qui n'avaient pas été éteints ou qui étaient mis en veille ont été infectés. Le centre s'est rendu compte de cette attaque le lundi matin lorsqu'un membre du personnel a signalé ne pas pouvoir ouvrir une session pour se connecter au système. Un message électronique de rançon se trouvait sur le bureau de l'ordinateur et dans chacun de ses fichiers indiquant que les fichiers étaient cryptés et énonçant les modalités de la rançon.

> « Je n'avais pas eu de migraine depuis des années, mais j'en ai eu un méchant toute une après cet incident. »

Le centre s'est immédiatement déconnecté de l'Internet. Selon l'enquête effectuée, l'accès s'est fait auprès d'un serveur de terminaux Windows 2003 désaffecté qui était censé être hors ligne était resté connecté au réseau. Il y avait également une politique de pare-feu permettant une connexion de bureau à distance (RDP) sur le serveur par Internet sans connexion à un réseau privé virtuel (RPV). Le protocole lié à la connexion de bureau à distance est un protocole relatif aux communications sur réseau conçu en vue de la gestion et de l'accès à distance aux bureaux, aux applications et au serveur de terminaux RDP.

Les pirates ont obtenu l'accès à l'ensemble du réseau par le biais du serveur sur lequel était installé Windows 2003. Ils se sont envoyé un mot de passe pour administrateur et ont procédé au chiffrement de tous les serveurs. Le chiffrement s'est ensuite propagé à tous les ordinateurs qui n'étaient pas éteints ou qui étaient mis en veille. Les copies de secours qui se trouvaient sur le réseau ont également été chiffrées.

Le centre utilisait le logiciel de dossier médical électronique (DME) *Nightingale on Demand* auquel l'accès était sécurisé sur Internet, ce qui a protégé les données médicales des clients. Le centre avait aussi adopté Office 365, une série d'applications infonuagiques, donc les fichiers Office (y compris les courriels) stockés en nuage n'ont pas été touchés. Seuls les fichiers locaux de l'organisation et les fichiers financiers ont été chiffrés par le rançongiciel.

Heureusement que, six ans auparavant, le fournisseur externe de technologies de l'information (TI) avait recommandé la création automatique régulière de copies de secours effectuée sur un réseau local virtuel séparé (réseau VLAN). Un réseau VLAN est un groupe de dispositifs sur un ou plusieurs réseaux locaux (LAN) configurés pour communiquer comme s'ils étaient reliés au même réseau même s'ils ne le sont pas. Effectuées depuis les six dernières années, les copies de secours se sont avérées très utiles, car après avoir vérifié que les fichiers n'avaient pas été touchés, le centre les a utilisées pour restaurer leurs systèmes.

Assurances

Le centre n'a pas eu à faire appel à leur compagnie d'assurance, puisqu'il a pu restaurer entièrement son système. Il a par contre déposé un rapport de police et informé le conseil

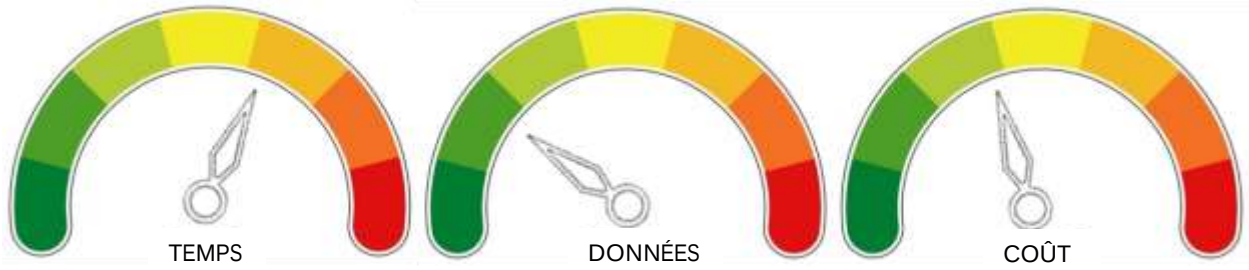
d'administration des données perdues, du coût global et de leurs suggestions en matière d'atténuation à cet égard.

Coût

Le coût était surtout lié au temps des membres du personnel, y compris les membres ayant travaillé directement à la restauration et au travail considérable de remise en état qui a dû être effectué.

Chronologie

Jour 1	À la fin de la journée, certains membres du personnel n'ont pas éteint leur ordinateur, d'autres ont mis le leur en veille et les autres ont arrêté le leur.
Jour 2	Un serveur sur lequel était installé Windows 2003 a fait l'objet d'une cyberattaque et a été utilisé pour accéder au reste du réseau, ce qui a fait que tous les ordinateurs n'ayant pas été éteints ou ayant été mis en veille ont été cryptés.
Jour 3	
Jour 4	Les utilisateurs ont été incapables de se connecter au réseau. Immédiatement, l'enquête a été lancée et les efforts de restauration ont commencé. Malheureusement les copies de secours stockées sur un serveur de stockage en réseau NAS avaient été chiffrées. Un processus de copie de secours installé sur un serveur séparé n'avait pas été touché. Les activités de restauration et de reconstruction ont commencé.
Jour 5	Certains utilisateurs ont obtenu l'accès au DME afin de pouvoir continuer à servir les clients.
Jour 6 – et suivants	Reprise complète des activités.
ACTUELLEMENT	Des mesures préventives ont été prises pour contrer la faiblesse en matière de sécurité que l'incident a révélée.



Étude de cas nº 2

Détails de la cyberattaque

La cyberattaque contre cet organisme est survenue un jeudi matin. Les pirates ont eu recours à une attaque par force brute pour accéder aux serveurs de l'organisme par le biais d'un protocole de serveur de bureau à distance (RDP) vulnérable. Une fois l'accès obtenu, les pirates ont inséré un rançongiciel qui a empêché quiconque d'accéder au système. Les pirates ont également pu accéder aux copies de secours conservées sur deux serveurs locaux, puis supprimer ces copies. Cet organisme avait lui aussi un protocole de sauvegarde infonuagique de tout le système. Or, le centre a découvert une faille importante de ce protocole : la base de données était devenue si importante que les copies ne se faisaient plus, et ce, malgré aucun avis donné au centre et aucun suivi de la part du fournisseur. On a ensuite découvert que les dernières copies de secours avaient été effectuées six semaines complètes avant l'incident, ce qui était dévastateur. Ce centre avait des DME locaux dont les données devaient faire l'objet de copies de secours. Tous les autres fichiers étaient conservés en nuage par l'entremise d'Office 365 et sont donc demeurés accessibles.

Heureusement, on avait demandé au centre neuf jours auparavant de transférer une copie complète de leur DME au fournisseur lequel s'occupait du transfert dans le cadre de la transition des DME. Bien que cela était beaucoup mieux que de perdre plus des données d'au moins 40 jours de travail, au cours de la période de neuf jours, le centre avait fait le ménage des données, et tout ce travail a été perdu. Le centre a également dû engager d'importants frais pour la réinstallation, la reconstruction et la restauration de l'environnement logiciel des DME locaux.

Assurances

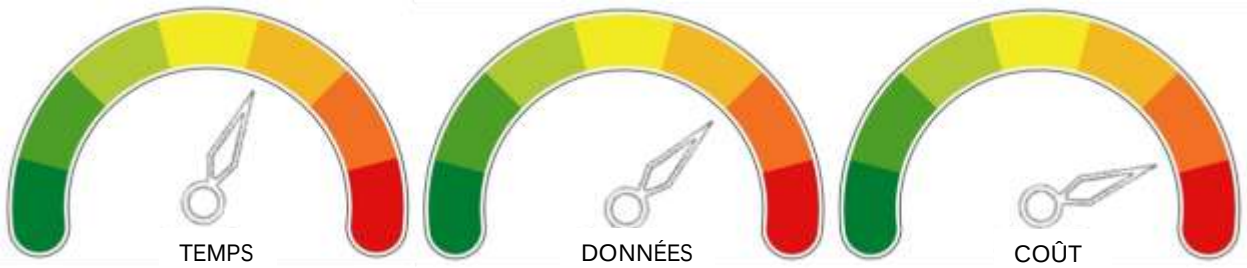
Le centre n'a pas fait appel à sa compagnie d'assurance, car il avait refusé l'assurance cybersécurité complémentaire quelques semaines auparavant. Le conseil d'administration et les clients ont toutefois été informés de la cyberattaque.

Coût

Le centre estime que le fait d'avoir des DME locaux a grandement contribué à l'augmentation du coût de restauration, car la réinstallation des DME ne pouvait être accomplie sans l'intervention du fournisseur de DME et du fournisseur des TI. Les autres frais ont été liés au temps du personnel et des frais d'avis aux clients. Ces coûts comprenaient également le travail direct de restauration et le travail de suivi considérable qui devait être accompli. Le centre estime que les coûts se sont élevés à environ 60 000 $.

Chronologie

Jour 1	Une attaque par force brute a permis l'accès au système suivi d'une infection immédiate par rançongiciel. Le centre découvre que les copies de secours ont été supprimées et que le processus de sauvegarde en ligne avait échoué six semaines complètes auparavant sans que le fournisseur envoie d'avis ou qu'un message d'erreur soit envoyé au moyen des processus du système.
Jour 2	Le centre décide d'utiliser la copie de secours du système au complet qui était utilisée aux fins des tests sur la migration des données (depuis seulement neuf jours).
Jour 3	La réinstallation, la reconstruction et la restauration des DME commence.
Jour 4	
Jour 5	
Jour 6	Accès très limité aux DME.
Jour 7 et suivants	Reprise complète des activités.
ACTUELLEMENT	Des mesures préventives ont été prises pour contrer la faiblesse en matière de sécurité que l'incident a révélée.



Étude de cas nº 3

Détails de la cyberattaque

Le centre a été avisé de la possibilité qu'une cyberattaque soit survenue lorsqu'un membre du personnel a indiqué ne pas pouvoir ouvrir un document. Une enquête a révélé que tous les documents partagés étaient sauvegardés avec des noms longs. Le réseau a été rapidement déconnecté de l'Internet, puisque l'on soupçonnait qu'une cyberattaque soit survenue. Il a ensuite été découvert que tous les fichiers faisant l'objet de partage réseau avaient été chiffrés. Chaque fichier contenait un seul fichier texte faisant état de la présence d'un rançongiciel ainsi que des instructions sur le paiement.

Le centre avait en place un système de sauvegarde à deux niveaux, l'un qui utilisait un lecteur de disque dur externe pour la sauvegarde de tous les documents sur un partage réseau et personnel. L'autre niveau consistait en un système à bande magnétique contenant une copie de secours du serveur Exchange et de tous les courriels. Malheureusement, il a été déterminé que le lecteur de disque dur externe avait cessé de faire des copies de secours plus de deux mois avant l'incident, ce qui signifiait que la dernière bonne copie de secours remontait à 60 jours auparavant. Aucune alerte n'avait signalé ce problème au centre. Les copies sur bandes magnétiques n'ont pas été atteintes. Les données financières et des DME étaient sauvegardées en nuage et n'ont donc pas été touchées.

> « Vous devez connaître à fond vos systèmes et leur architecture. »
>
> - Administrateur de système

Une décision a été prise d'entrer en contact avec les pirates, qui ont répondu quelques heures plus tard en demandant plus de détails (nombre de machines atteintes, taille de l'organisation, système d'exploitation des serveurs). Se rendant compte qu'ils avaient alerté les pirates de l'existence d'une victime potentielle (ce qui pourrait avoir une incidence sur le montant de la rançon demandée), le centre a immédiatement bloqué l'adresse courriel et du domaine. En effectuant un retour sur les dommages, il a été décidé de supprimer tous les fichiers cryptés et d'utiliser la toute dernière bonne copie de secours effectuée deux mois auparavant. Cette décision a été prise assez rapidement, puisque le nombre de dossiers créés par les utilisateurs au cours de cette période était relativement peu élevé. Quelques heures après la cyberattaque, les activités du centre ont repris.

Au cours de l'analyse de la cause principale de l'incident, on a découvert l'existence d'un serveur sur lequel était installé Windows 2003 et qui était configuré pour l'accès à distance par Internet. Il semblerait qu'un ancien administrateur de système utilisait ce serveur aux fins d'administration hors site. L'administrateur actuel n'était pas au courant de cet accès, car il n'existait aucun document lié à l'ancienne infrastructure du système. Les pirates ont pu obtenir un accès non autorisé au réseau par le biais de ce serveur.

Assurances

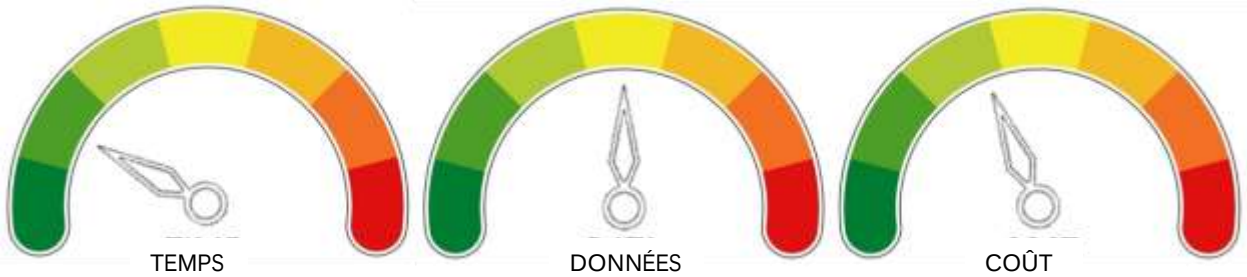
Le centre a fait appel à sa compagnie d'assurance qui a répondu qu'elle n'interviendrait pas, étant donné qu'il n'y avait pas de négociation en cours avec les pirates.

Coûts

Le coût était lié au temps du personnel ayant travaillé directement à la restauration pendant une journée complète.

Chronologie

Jour 1	5 h – La cyberattaque commence : tous les fichiers du réseau sont cryptés. 8 h – La cyberattaque est découverte et le centre est déconnecté du réseau. 13 h – Le centre décide de supprimer les fichiers cryptés et d'utiliser la copie de secours effectuée deux mois auparavant.
Jour 2 et suivants	Reprise complète des activités avec perte de fichiers ayant été créés au cours de la période de deux mois.
ACTUELLEMENT	Des mesures préventives ont été prises pour contrer la faiblesse en matière de sécurité que l'incident a révélée.



Étude de cas nº 4

Détails de la cyberattaque

Contrairement aux autres centres faisant l'objet des quatre études de cas aux présentes, ce centre ne dispose d'aucun personnel des TI sur les lieux pouvant comprendre et gérer les cyberattaques. Le centre était passé d'un fournisseur privé de TI à un fournisseur de TI situé dans un hôpital. La mise en œuvre d'un plan TI proposé par son fournisseur actuel était en cours et devait s'échelonner sur une période de trois ans. Un des éléments de ce plan était de déménager un des systèmes du centre, dont une copie de secours était en cours au centre, à l'hôpital pour que les copies de secours soient effectuées hors site. Entre temps, le nouveau fournisseur de TI avait recours aux copies de secours effectuées au centre. Or, ces copies n'étaient pas effectuées sur un serveur indépendant.

La cyberattaque a été lancée lorsqu'un utilisateur a cliqué sur un lien menant vers un rançongiciel. Le centre s'est aperçu peu après que personne n'avait accès à ses courriels.

> « Si vous changez de fournisseur, veillez à ce qu'il y ait un transfert adéquat des responsabilités. »

Le centre a contacté le fournisseur de TI en toute urgence. Ce dernier a constaté que le serveur Exchange avait été infecté par rançongiciel. Le fournisseur a également constaté que les copies de secours locales avaient elles aussi été cryptées. Le directeur général s'est souvenu que le fournisseur précédent avait créé un processus de copies de secours en cas de sinistre sur un serveur indépendant et a demandé au fournisseur actuel d'effectuer une vérification à cet égard, ce qui a malheureusement pris presque trois jours. Chaque fournisseur a jeté le blâme sur l'autre, après quoi le centre a pu restaurer son environnement.

Le directeur général recommande à tous de veiller à ce que tout nouveau fournisseur connaisse bien l'infrastructure du réseau de l'organisation. Il est également hautement recommandé que les centres mettent à l'essai leur plan de continuité des activités (PCA) et leur plan de reprise après sinistre (PRAS).

Assurances

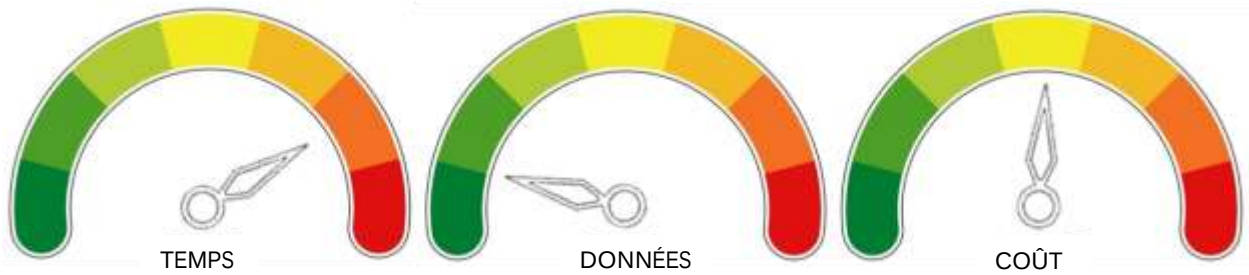
Le centre a fait appel à sa compagnie d'assurance qui a répondu qu'elle n'interviendrait pas, étant donné qu'il n'y avait pas de négociation en cours avec les pirates.

Coût

Le coût était lié au temps du personnel, y compris le personnel travaillant directement à la restauration et au travail considérable de suivi devant être effectué. Le personnel du centre a dû utiliser les télécopieurs et les téléphones, puisqu'il n'avait pas accès aux courriels au cours de cette période.

Chronologie

Jour 1	Les membres du personnel cliquent sur un lien qui engendre l'infection du système. Même si la connexion physique au réseau a été rapidement coupée, cela n'a pas été effectué assez rapidement pour prévenir une perte d'accès au serveur Exchange. Le centre a communiqué avec le fournisseur de TI.
Jour 2	Aucune réponse du fournisseur de TI.
Jour 3	
Jour 4	
Jour 5	Le fournisseur de TI actuel commence à travailler sur la restauration du système, mais constate que ce système n'a pas été bien configuré.
Jour 6	Les fournisseurs de TI actuels et précédents travaillent à la restauration du système.
Jour 7	
Jour 8 et suivants	Reprise complète des activités.
ACTUELLEMENT	Des mesures préventives ont été prises pour contrer la faiblesse en matière de sécurité que l'incident a révélée.



Conclusion et leçons tirées

Dans tous les cas à l'étude, les pirates cherchaient à crypter les données plutôt qu'à carrément les voler. Bien qu'aucune de leurs activités n'ait laissé croire que des données avaient été transférées des réseaux locaux, il s'agit d'une tendance croissante. Les pirates cryptent ou suppriment les données après les avoir copiées. Ensuite, soit qu'ils exigent une rançon ou qu'ils vendent les données à d'autres parties intéressées. Les centres dont les dossiers médicaux électroniques (DME) sont sauvegardés en nuage et ceux qui ont procédé à une migration vers des systèmes infonuagiques Office, par exemple Office 365, ont été protégés contre une cyberattaque de cryptage ciblant leurs systèmes.

Les pirates peuvent obtenir l'accès à vos systèmes par le simple fait d'avoir réussi à deviner une seule fois. Or, il est important que les mesures de défense de votre centre protègent vos systèmes en tout temps. Protéger votre centre contre de telles cyberattaques et renforcer la cyber-résilience de votre organisation ne peut être assuré qu'en ayant recours à une approche systématique à plusieurs niveaux. Voici neuf des principales leçons à tirer :

- Le premier niveau d'atténuation est **d'appliquer** promptement des correctifs logiciels **et d'utiliser des technologies** qui contrent les programmes malveillants afin de bloquer, ou du moins de détecter, les infections par de tels programmes. Désactivez tout service redondant et activez les coupe-feux.

- Limitez **les types de tâches qu'effectue l'administrateur de système sur le serveur de** secours qui pourraient le rendre vulnérable. Les administrateurs de système ne devraient jamais se trouver sur l'Internet directement à partir de l'appareil sur lequel sont effectuées les copies de secours, et surtout pas à partir d'un compte d'utilisateur privilégié sur cet appareil.

- **Connaissez bien l'infrastructure de votre réseau** – des serveurs oubliés ou dont on ignorait l'existence ont fait l'objet de cyberattaques dans deux des cas examinés. Étant donné que de nombreuses cyberattaques sont possibles par l'entremise du protocole de bureau à distance (PBD), il est toujours opportun de désactiver l'accès externe à celui-ci. Si votre organisation utilise le PBD dans le cadre de ses activités, envisagez d'y appliquer un coupe-feu interne. Par exemple, limitez l'accès au PBD uniquement aux membres du personnel ayant validé leur identité et utilisant un RPV pour accéder au réseau.

- Sensibilisez les utilisateurs. Dans tous les cas examinés, des cyberattaques par rançongiciel ont pu survenir parce qu'un serveur Windows n'était pas protégé, l'infection s'est ensuite propagée au reste du réseau, ou ont été initiées en raison d'actes par inadvertance d'un utilisateur sur le réseau. Adoptez des politiques « d'utilisation informatique acceptable » et sensibilisez les utilisateurs quant à l'importance d'agir prudemment en ligne et de rester vigilants lorsqu'ils utilisent la technologie.

- **Veillez à ce que la haute direction et le conseil d'administration de votre** organisation soient au fait de tout risque en matière de technologie, des mesures

d'atténuation des risques et du coût de ces mesures. **Cela s'applique particulièrement** aux centres plus modestes ayant des ressources limitées. Il est essentiel pour toutes les organisations de communiquer ces renseignements, car les données sont devenues des marchandises. La supervision de la part du conseil d'administration et l'élaboration de politiques sur la responsabilisation de la haute direction sont des éléments fondamentaux de la création d'une culture de sensibilisation et de gestion en matière de cyberrisque.

- Le dernier et plus essentiel moyen de protection est le système de secours. Assurez-vous qu'il est le premier des systèmes à faire l'objet de mesures correctives. Séparez les systèmes de secours autant que possible. Ceci signifie de ne pas utiliser Active Directory pour ouvrir une session afin de vous connecter au serveur de secours. Il est aussi important que le système de secours soit sur un réseau séparé ou un réseau VLAN, ce qui minimisera le risque qu'un programme malveillant n'infecte le réseau à la recherche d'autres systèmes à compromettre.

- Examinez les avantages de souscrire une assurance cybernétique, également désignée assurance cyberrisque ou couverture d'assurance cyberresponsabilité. Ces polices d'assurance ont été conçues pour aider les organismes à atténuer le risque en assumant les frais de récupération à la suite d'une atteinte à la cybersécurité ou d'un incident similaire. Familiarisez-vous avec votre police d'assurance cybernétique et ce qu'elle couvre. Une police d'assurance cybernétique pourrait couvrir les pertes pécuniaires causées par le temps d'arrêt du réseau, l'interruption des activités, la récupération des données perdues et du coût de gestion de la crise, y compris le redressement de la situation en cas d'atteinte à la réputation. La police pourrait également comprendre la couverture d'honoraires juridiques associés à la publication de renseignements confidentiels ou à la propriété intellectuelle, aux règlements judiciaires, aux amendes règlementaires et aux frais liés à la cyberextorsion, comme c'est le cas avec les rançongiciels[4].

- Les autorités provinciales et territoriales ainsi que le Centre canadien de la cybersécurité conseillent de ne pas payer de rançon[5] laquelle ne garantit pas que la clé de décryptage fonctionnera ou que l'organisme restera à l'abri de cyberattaques ultérieures ou ne fera plus l'objet de tentatives d'extorsion. Toute rançon payée ne fait qu'encourager les criminels et faire en sorte qu'ils profitent de ces activités.

- **La cybersécurité n'est pas une question liée uniquement aux technologies de l'information.** Il s'agit d'une question devant être abordée en matière de gestion du risque intégré et de la restauration dans le cadre du programme global de continuité des activités et de reprise après sinistre de votre organisme.

[4] Healthcare Insurance Reciprocal of Canada https://www.hiroc.com/
[5] https://www.cse-cst.gc.ca/fr/backgrounder-fiche-information

Annexes

- L'Alliance pour des communautés en santé publie mensuellement des bulletins sur la protection et la sécurité des données. Veuillez visiter notre portail pour membres où vous trouverez tous nos bulletins. Notre portail pour membres se trouve à l'adresse suivante : https://aohc.site-ym.com/members/group_content_view.asp?group=141556&id=529385
- Neufs éléments dont il faut tenir compte dans le cadre de la préparation contre les cyberattaques
- Plan d'intervention en cas d'incident
- Liste de contrôle – Intervention immédiate en cas de cyberattaque
- Glossaire

Neuf éléments dont il faut tenir compte dans le cadre de la préparation contre les cyberattaques

ACTION	DESCRIPTION
Antivirus et privilèges liés au réseau	De nos jours, le fait d'utiliser un antivirus comme seule solution ne suffit plus. Configurez le système pour qu'il autorise des partages réseau et autorisations utilisateur. Un privilège permet à un utilisateur d'effectuer une tâche.
Données de secours	Dans l'éventualité où une attaque surviendrait, il est possible de couper l'alimentation du système, de le réimager et de le réinstaller en utilisant les données de la dernière copie de secours. Il est possible de récupérer toutes les données de votre dernière copie de secours. Or, cela suppose que le rançongiciel n'a pas infecté et chiffré vos données de secours. Discutez avec vos experts des TI pour savoir quelles stratégies devraient être mises en œuvre pour sécuriser vos copies de secours. Il est également essentiel de vérifier que vos copies de secours automatisées continuent de se faire. Vous pouvez même effectuer un test de restauration pour vous assurer de l'intégrité et de la validité des données. Il est tout aussi important de valider vos copies de secours que de les configurer.
Sensibiliser les utilisateurs	Les maillons les plus faibles dans toute chaîne de sécurité sont les gens. Vous pouvez aider les utilisateurs à détecter les tentatives d'hameçonnage et les programmes malveillants envoyés par courriel, ce qui contribuera à protéger votre réseau.
Surveiller les activités sur le réseau	Vous pouvez déceler des cyberattaques lorsque vous êtes en mesure de voir tout ce qui se passe sur votre réseau. Surveiller l'utilisation de la bande passante, la vitesse du réseau et les activités dans la base de données peut vous aider à détecter toute anomalie.
Appliquez les correctifs	Il est essentiel que les logiciels soient mis à jour régulièrement. Le fait d'apporter des correctifs aux logiciels de tiers exploités couramment déjouera de nombreuses attaques. Il devrait être interdit aux utilisateurs de reporter l'application de correctifs, car il est prouvé que de reporter leur application augmente le risque de faire l'objet d'une cyberattaque.
Prévenir l'infiltration aisée	La plupart des infections par rançongiciel sont introduites au moyen de l'envoi d'une pièce jointe à un courriel ou du téléchargement d'un programme malveillant. Bloquez avec diligence les sites Web, les courriels et les pièces jointes malveillants en ayant recours à une approche de sécurité à plusieurs niveaux.
Protéger le réseau	Adoptez une approche à plusieurs niveaux, dont chacun comporte des éléments de sécurité.
Payer la rançon uniquement	N'envisagez de payer la rançon que comme solution de dernier recours. Par ailleurs, sachez qu'il n'est pas garanti que vous retrouviez vos données et que le fait de payer la rançon ne fait que motiver les cybercriminels à lancer une autre attaque. Faites intervenir votre

en dernier recours	compagnie d'assurance, car elle peut vous aider lors de ce processus, si vous choisissez cette option.
Segmenter le réseau	Limitez les ressources auxquelles les pirates peuvent avoir accès. En exerçant un contrôle dynamique en tout temps, vous veillez à ce que le réseau tout entier ne soit pas compromis lors d'une seule attaque.

Plan **d'intervention en cas d'incident**

ÉLÉMENT	MESURE	NOTES
Gestion de l'équipe d'intervention	Identifiez les membres de l'équipe d'intervention et leurs tâches respectives.	L'équipe d'intervention devrait comprendre au moins : - Un chef d'équipe d'intervention en cas d'incident - Un membre de la haute direction - Un expert du problème en cause du système d'information
Copies de secours et tests liés à la restauration	Validez vos données de secours	- Veillez à ce qu'une copie de secours de tous les systèmes critiques soit effectuée et que ceux-ci soient maintenus hors ligne et hors site afin de les protéger de toute cyberattaque éventuelle. - Effectuez périodiquement des tests de restauration des données à partir de vos copies de secours pour vérifier l'intégrité des données et valider que le processus de copie de secours fonctionne bien.
Politique d'interruption	Validez et communiquez votre politique d'interruption d'accès aux DME	Comment le flux du travail est-il modifié si votre centre n'a qu'un accès limité, ou aucun accès, à l'Internet et aux DME?
Plan de communication	Lancez votre plan de communication	- Déterminez ce qui se produirait si les moyens de communication habituels étaient compromis, p. ex. par courriel. - Qui doit le savoir et comment? - Qui s'adressera aux médias? Quels sont les messages clés?
Plan juridique	Déterminez quelles sont vos obligations sur le plan juridique	- Établir quels organismes règlementaires doivent être informés en cas d'atteinte aux données ou de perte de données. - Établir quelles communications doivent être envoyées aux clients. - Déterminer si le commissaire à la protection de la vie privée doit en être informé.
Assurances	Vérifiez si vous avez une couverture d'assurance et ce qui est couvert	Les polices responsabilité générale et biens ne couvrent pas toutes les pertes financières liées aux cyberincidents. Dans certaines situations, il est nécessaire de souscrire une assurance cyberrisque distincte. Vérifiez vos polices d'assurance et les limites de couverture pour vous assurer qu'elles sont opportunes et adéquates, et que vous respectez les exigences prévues dans votre politique.

Liste de contrôle – Intervention immédiate en cas de cyberattaque

Gestion de l'incident		
☐	Contactez l'équipe d'intervention en cas d'incident.	
☐	Lancez le plan de communication en cas d'incident.	
☐	Communiquez avec votre compagnie d'assurance, au besoin.	
☐	Communiquez avec les organismes de règlementation, au besoin.	
☐	Communiquez avec les clients, au besoin.	
☐	Communiquez avec le commissaire à la protection de la vie privée, au besoin.	

Tout déconnecter		
☐	Déconnectez votre ordinateur du réseau.	
☐	Éteignez toute fonctionnalité sans fil : Wi-Fi, Bluetooth, communications en champ proche.	
☐	Communiquez avec votre fournisseur ou vos experts en TI.	
☐	Communiquez avec le personnel d'Alliance.	

Évaluez l'étendue de l'infection		
☐	Les lecteurs mappés ou partagés sont compromis.	
☐	Les fichiers mappés ou partagés d'autres ordinateurs sont compromis.	
☐	Tout type de périphérique de stockage en réseau	
☐	Disques durs externes	
☐	Tout type de clé USB	
☐	Stockage infonuagique : Dropbox, Google Drive, OneDrive, etc.	
☐	Applications qui auraient pu être atteintes.	
☐	Assurez-vous que les systèmes qui n'ont pas été atteints demeurent protégés.	

Déterminez de quel type de rançongiciel/virus il s'agit		
☐	Quel type de rançongiciel/virus s'agit-il? Par exemple, CryptoWall, Teslacrypt, Dharma, etc.	

Détermination du type d'intervention

Option 1 – Restauration à partir de la copie de secours non chiffrée		
☐	Trouvez vos copies de secours.	
☐	Vérifiez l'intégrité des copies de secours.	
☐	Vérifiez s'il existe des versions précédentes de fichiers qui pourraient être stockées en nuage.	
☐	Supprimez le rançongiciel de votre système infecté.	
☐	Restaurez vos fichiers en utilisant les copies de secours.	
☐	Trouvez le vecteur d'infection et protégez votre système contre des cyberattaques ultérieures.	

Option 2 – Solution de décryptage		
☐	Dans la mesure du possible, déterminez le type de virus dont il s'agit et sa version.	
☐	Trouvez un décrypteur en ligne; cependant, il est possible qu'il n'en existe pas pour les virus les plus récents.	
☐	Si vous réussissez à en trouver, y joindre tout support de stockage contenant des fichiers chiffrés (disques dur, clés USB, etc.).	
☐	Décryptez les fichiers.	
☐	Déterminez le vecteur et le pseudonyme du virus.	

Option 3 – Ne rien faire (perte de fichiers)		
☐	Supprimez le rançongiciel.	

Après l'incident

☐	Examen après l'incident et toute modification devant être apportée au plan d'intervention en cas d'incident mettant en cause la cybersécurité, selon l'expérience vécue et l'analyse de l'incident.	
☐	Analyse de la cause principale, y compris la documentation des faits, des constatations, des activités, des résultats et des recommandations de mesures d'atténuation, le cas échéant.	
☐	Préparation d'un rapport sur l'incident et les leçons tirées.	

Liste de contrôle – Prévention contre les rançongiciels

Se protéger à l'avenir		
☐	Offrir aux utilisateurs une formation sur la sécurité efficace pour qu'ils sachent quoi surveiller afin d'éviter le téléchargement et l'exécution d'applications malveillantes de la part de criminels.	
☐	Effectuer des simulations d'hameçonnage pour que les utilisateurs se familiarisent avec les menaces qui existent actuellement.	
☐	S'assurer que le pare-feu fonctionne et que la configuration est sécurisée.	
☐	Mettre en place des filtres antipourriel et antihameçonnage, ce qui peut être accompli en installant des logiciels ou du matériel tel que des dispositifs comme SonicWALL ou Barracuda (ou autres).	
☐	Veiller à ce que tous les membres de l'organisation utilisent la dernière version de leur logiciel antivirus ou d'autres produits de protection des dispositifs d'extrémité comme l'établissement d'une liste blanche ou de fichiers exécutables de blocage en temps réel.	
☐	Mettre en place des politiques restrictives relatives aux logiciels (notamment désactiver les ports USB, l'exécution automatique, etc.) sur votre réseau afin d'empêcher l'exécution d'applications. (*facultatif*)	
☐	Mettre en place une procédure stricte relative aux mesures correctives pour la mise à jour de toutes les applications.	
☐	Mettre en place une solution logicielle ou de matériel, ou une combinaison des deux, pour que soient effectuées des copies de secours.	
☐	S'assurer que des copies de secours ont été faites de toutes les données auxquelles vous devez avoir accès ou sauvegarder, y compris les dispositifs de stockage mobiles et USB.	
☐	Veiller à ce que vos données soient en sécurité, redondantes et facilement accessibles une fois qu'une copie de secours en a été faite.	
☐	Effectuer régulièrement des tests des procédures de copie de secours et de restauration. Vérifier l'intégrité des données des copies de secours physiques et s'assurer que les données faisant l'objet de copies de secours faites en ligne ou sur logiciels peuvent facilement être restaurées.	

Glossaire

TERME	DÉFINITION
Attaque par force brute	Attaque par force brute est une tentative de trouver des renseignements comme un mot de passe ou un numéro d'identification personnelle (NIP) au moyen d'un processus d'essais et d'erreurs.
Piège à clics	Contenu dont le but principal est d'attirer l'attention et d'encourager les visiteurs à cliquer sur un lien qui mènera vers une page Web quelconque.
Cryptage / chiffrement	Le processus de conversion en code d'informations ou de données afin d'empêcher d'y accéder (*sans autorisation*).
RLE	Un réseau local d'entreprise (RLE ou LAN) est un réseau d'ordinateurs et d'appareils liés qui utilisent une ligne de communication commune ou un lien sans fil commun vers un serveur. Habituellement, un RLE (ou LAN) comporte des ordinateurs et des périphériques connectés à un serveur situés dans un endroit distinct comme un bureau. Les ordinateurs et autres appareils mobiles utilisent un RLE (ou LAN) pour partager des ressources comme une imprimante ou un espace de stockage sur le réseau.
Programme malveillant	Tout logiciel conçu pour être implanté dans un système informatique avec l'intention d'en perturber le fonctionnement ou de perturber le fonctionnement des ordinateurs ou de les endommager.
Privilèges d'accès au réseau	Selon le concept de privilèges d'accès au réseau, les utilisateurs ne sont autorisés qu'à faire certaines choses. Par exemple, un utilisateur ordinaire ne peut habituellement pas modifier les fichiers du système d'exploitation, tandis qu'un administrateur de système est habituellement autorisé à le faire, puisque cela fait partie de l'entretien du système informatique.
Hameçonnage	Tentative d'escroquerie consistant à envoyer massivement un courriel, apparemment émis par des entreprises réputées, dans le but d'obtenir des renseignements confidentiels comme des mots de passe et des numéros de cartes de crédit.
Rançongiciel	Type de programme malveillant qui empêche les utilisateurs d'avoir accès à leur système ou à leurs fichiers personnels, et qui demande le paiement d'une rançon pour en retrouver l'accès.
Serveur distant	Genre de serveur qui offre une série de services permettant aux utilisateurs de se connecter à distance en utilisant le réseau ou l'Internet. Une fois connecté au serveur distant, un utilisateur peut avoir accès à ses données, à son bureau et à ses applications en plus de pouvoir imprimer et utiliser d'autres services supportés.
RDP	Protocole exclusif de Microsoft, protocole de bureau à distance (RDP), qui fournit une interface graphique à l'utilisateur au moyen de laquelle il peut se connecter à un autre ordinateur par la connexion à un réseau.
Faux logiciels antivirus	Logiciel malveillant potentiellement dangereux, comme de faux logiciels antivirus, qui effraie l'utilisateur en prétendant que son ordinateur est la proie d'une menace dans le but d'inciter ce dernier à l'acheter et à en entamer le téléchargement.
Verrouilleurs d'écran	Rançongiciel qui pourrait vous demander de confirmer une information sur un site Web et qui verrouille votre écran tout en affichant un message dans lequel on demande habituellement un paiement. Votre système d'exploitation est complètement verrouillé avec ce type de rançongiciel.

TERME	DÉFINITION
Harponnage	Pratique frauduleuse consistant en l'envoi de courriels qui semblent provenir d'une source connue ou de confiance visant à faire en sorte que des personnes ciblées donnent des renseignements confidentiels. Contrairement à l'hameçonnage traditionnel, le harponnage est très ciblé. Le message ne sera envoyé qu'à une seule ou qu'à quelques personnes soigneusement choisies. L'objectif est de déterminer qui en sera la cible.
Logiciel espion	Logiciel destiné à obtenir, à l'insu de l'utilisateur, des données confidentielles sur les activités effectuées sur un autre ordinateur à partir du disque dur de celui-ci.
TOR	Logiciel gratuit qui permet de communiquer de façon anonyme.
Réseau VLAN	Groupe d'appareils sur un ou plusieurs réseaux locaux configurés pour communiquer comme s'ils étaient reliés au même routeur alors qu'en réalité, ils sont situés dans plusieurs différents segments du réseau local.
RPV (ou communément VPN)	Réseau privé pouvant être utilisé dans un réseau public permettant aux utilisateurs d'envoyer et de recevoir des données sur des réseaux public ou de partage de la même manière que si leur appareil était directement connecté au réseau privé.