TRAVELERS

Mémoire de Travelers sur les cyberrisques

Votre entreprise n'est pas à l'abri. Les cybercriminels testent vos mécanismes de défense. Ils scrutent vos faiblesses. Leur but est de compromettre votre réseau, de vider vos dossiers de sauvegarde et de chiffrer vos systèmes et vos données. Votre entreprise est-elle prête?

L'an dernier, une firme de sécurité a détecté à elle seule plus de 187 millions d'attaques par rançongiciels. La plupart de ces attaques échouent, mais celles qui réussissent sont de plus en plus perverses.[1]

Les cybercriminels ne se contentent plus d'exiger de modestes rançons après avoir compromis un réseau. Ils demandent désormais des montants à six, sept, voire huit chiffres. Selon les données du service des Réclamations de Travelers, le nombre de demandes de règlement pour attaque par rançongiciel enregistrées en 2019 était quatre fois supérieur à celui de 2017, tout comme la gravité des pertes connexes.

Pour obliger les entreprises à payer des sommes exorbitantes, les utilisateurs de rançongiciel sont de plus en plus agressifs. Ils s'infiltrent plus loin dans les réseaux de leurs victimes pour accéder à leurs systèmes et à leurs données critiques. Ils vident leurs dossiers de sauvegarde et, dans certains cas, menacent de divulguer leurs données sensibles ou confidentielles. Par conséquent, les entreprises ont de plus en plus de mal à se rétablir en cas d'attaque. Du troisième au quatrième trimestre de 2019, le temps d'indisponibilité moyen attribué à des attaques par rançongiciel est passé de 12,1 à 16,2 jours.[2] Aujourd'hui, ces attaques peuvent paralyser les entreprises prises au dépourvu, voire les forcer à fermer leurs portes.

À Travelers, notre objectif est d'aider les entreprises de toute taille et de tout secteur à gérer les cybermenaces existantes et émergentes, y compris les rançongiciels. Dans le présent Mémoire sur les cyberrisques, nous répondons aux questions les plus courantes sur ces derniers, dont la plus complexe, à savoir si les entreprises victimes de cybercrime doivent payer ou non la rançon demandée. Nous proposons également des mesures simples et rentables que les entreprises peuvent prendre pour mieux se protéger contre ces menaces, qui évoluent rapidement.

Nous croyons fermement que toutes les entreprises gagneront à en apprendre davantage et à être plus vigilantes.

PLEINS FEUX SUR LES RANÇONGICIELS

LE TEMPS D'INDISPONIBILITÉ

ATTRIBUABLE **À DES ATTAQUES PAR RANÇONGICIEL** A **TRIPLÉ** DE **2018** À **2019**.

Source : Datto, « Global State of the Channel: Ransomware Report »

Pour causer le plus de dommages possible, les criminels qui pénètrent à l'intérieur d'un réseau chiffrent toutes les données qui sont à leur disposition. Ils espèrent ainsi compromettre le réseau de leur victime pour qu'elle ne puisse pas se rétablir, la forçant ainsi à payer.

– Kevin Haley, Équipe d'intervention de HCL Technologies©

RANÇON : PAYER OU NE PAS PAYER

Les entreprises victimes d'une attaque par rançongiciel peuvent être confrontées à cette dure question : verser la rançon exigée ou non. Cette décision ne peut pas être prise à la légère et les entreprises, tout comme les attaques par rançongiciel, présentent chacune des particularités qui influenceront leur prise de position. Il faut donc faire appel à des professionnels compétents, dont des avocats et des experts en services judiciaires numériques qui ont l'expertise requise pour traiter de tels événements. Dans de nombreux cas, les coûts d'embauche de ces professionnels seront couverts par une assurance cyberrisques de Travelers.

Les points suivants doivent être attentivement évalués :

- L'entreprise peut-elle récupérer ses systèmes et ses données sans payer la rançon?
- Le paiement de la rançon réduira-t-il le coût de recouvrement global?
- Si la rançon est payée, les criminels fourniront-ils les clés requises pour déchiffrer les données?

Pour répondre à cette dernière question, il est important de solliciter les conseils de professionnels compétents. Les criminels ne fournissent pas toujours les clés de déchiffrement requises suite au paiement d'une rançon. Certains exigeront plus d'argent, tandis que d'autres refuseront tout simplement de collaborer. Les experts en services judiciaires numériques qui interviennent régulièrement en pareil cas peuvent aider les entreprises à décider si le paiement de la rançon en vaut la peine ou si cela poussera plutôt les criminels à redoubler de vigueur.

Des entreprises refusent de payer par principe.

La décision ultime, qui n'est pas facile à prendre, revient finalement aux victimes. Cependant, le soutien offert dans le cadre d'une police d'assurance cyberrisques de Travelers peut faire toute la différence.

ÉTUDE DE CAS

Que se passe-t-il après une attaque par rançongiciel? Chaque demande de règlement est unique, mais l'exemple ci-dessous permet d'illustrer ce qui peut arriver et comment se rétablir. La victime décrite ici est une entreprise de services professionnels qui compte 105 employés dans 3 succursales distinctes.

JOUR -60 : Les cybercriminels compromettent le réseau de la victime. Ils accèdent ainsi à un compte administrateur et explorent le réseau, sans être détectés, en utilisant le protocole d'accès de bureau à distance (RDP) pendant deux mois.

JOUR 0 : Peu après minuit, le rançongiciel « Ryuk » chiffre tous les serveurs de la victime. Les cybercriminels exigent 150 bitcoins (BTC), soit environ 600 000 $. La victime contacte Travelers et un appel a lieu le jour même en compagnie d'un avocat spécialisé en protection des données (« services juridiques ») et d'un cabinet de services judiciaires numériques (« services judiciaires »).

JOUR 1 : La victime a des sauvegardes, mais ses dossiers critiques ne peuvent pas tous être récupérés. À l'aide des services judiciaires embauchés, la victime parvient à négocier la réduction de la rançon à 80 BTC et obtient une « preuve de vie », à savoir la preuve que les cybercriminels seront en mesure d'annuler le chiffrement de ses données. Les services judiciaires commencent alors à sécuriser le réseau de la victime.

Apprenez des erreurs des autres. Vous ne vivrez pas assez longtemps pour toutes les faire vous-même.

– Eleanor Roosevelt

ÉTUDE DE CAS (SUITE)

JOUR 2 : Les services judiciaires assurent le paiement de la rançon négociée et obtiennent une clé de déchiffrement. Le processus de déchiffrement prend du temps, mais la plupart des données de la victime sont récupérées après une semaine. En tout, les initiatives de recouvrement s'échelonnent sur un mois.

JOUR 21 : Des services de protection contre l'usurpation d'identité et de surveillance du crédit sont offerts aux personnes dont les données personnelles étaient sauvegardées sur l'un des serveurs de la victime.

JOUR 86 : La victime rencontre Travelers pour présenter les améliorations qu'elle a apportées à ses mécanismes de sécurité et, peu de temps après, elle renouvelle sa police d'assurance CyberRisques Travelers.

À ce jour, plus de 400 000 $ ont été payés en règlement. Les dépenses couvertes comprennent le paiement de la rançon elle-même ainsi que le remboursement des frais d'avocat et des services judiciaires numériques, de récupération des données et d'usurpation d'identité et de surveillance du crédit. L'assurance cyberrisques peut également couvrir les pertes de revenus attribuables à l'interruption des activités et « l'amélioration », un nouveau type de protection qui aide les entreprises à renforcer leurs contrôles après une cyberattaque.

Pour des mesures simples et rentables de réduction des risques d'attaques par rançongiciel, consulter la page 5.

Nous assistons à un bouleversement : le nombre de demandes de règlement liées à des attaques par rançongiciel a connu une hausse vertigineuse au cours des dernières années.

– John Mullen, Mullen Coughlin, LLC

RANÇONGICIEL : CE QUE VOUS DEVEZ SAVOIR

Un rançongiciel, qu'est-ce que c'est?

Les rançongiciels sont des logiciels malveillants (« maliciels »). Les cybercriminels accèdent au réseau de leur victime pour s'emparer de ses données ou commettre des infractions. Ils peuvent également lancer une attaque par rançongiciel pour chiffrer ses systèmes informatiques et ses données. Ils demandent alors une rançon en échange d'une clé de déchiffrement.

Quelles entreprises sont à risque?

Les entreprises de toute taille et de tout secteur sont à risque. Les cybercriminels ne font généralement pas de distinction entre leurs victimes.

Les forces de l'ordre peuvent-elles aider les victimes de rançongiciel?

La GRC a créé le Groupe national de coordination contre la cybercriminalité (GNC3) en avril 2020. Ce groupe collabore principalement avec la police pour coordonner les enquêtes et partager des renseignements. Le GNC3 met aussi sur pied un nouveau système de signalement public.

RANÇONGICIEL : CE QUE VOUS DEVEZ SAVOIR (SUITE)

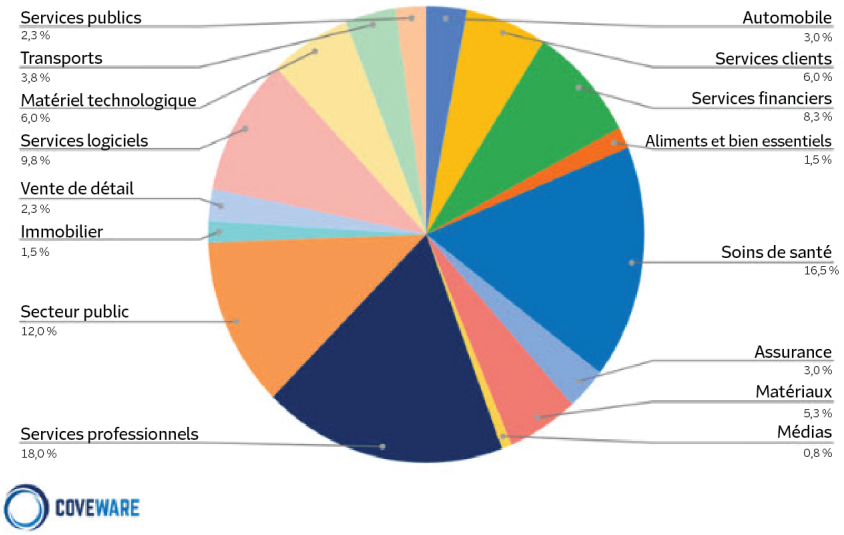
Comment les rançons sont-elles payées?

Les criminels demandent généralement à être payés en cryptomonnaie, ou en bitcoins. Pour payer une rançon, les victimes font habituellement appel à un tiers qui se charge des négociations et du paiement.

Y a-t-il une assurance pour les rançongiciels?

Oui. À Travelers, nous offrons une protection contre les rançongiciels qui couvre le paiement de la rançon elle-même, les coûts de récupération des données, la perte de revenu attribuable à l'interruption des activités et les frais d'avocat, de services judiciaires numériques et de relations publiques. Une couverture est également offerte pour « l'amélioration » afin d'aider les entreprises victimes d'attaque par rançongiciel à renforcer leurs contrôles. Pour de plus amples renseignements sur l'assurance cyberrisques, communiquez avec votre courtier ou votre courtière d'assurance.

Secteurs victimes d'attaques par rançongiciel au T3 de 2022[3]



UN RISQUE ÉMERGENT : LES FOURNISSEURS DE SERVICE

De nombreuses entreprises dépendent de fournisseurs de services TI pour gérer leurs réseaux et leurs systèmes, ces derniers leur offrant des technologies et des solutions dont la mise en œuvre interne ne serait pas rentable. Ce faisant, elles doivent connaître les risques auxquels elles s'exposent.

De plus en plus d'attaques par rançongiciel découlent de la compromission des biens desdits fournisseurs de services TI. Pour atténuer ce risque, les entreprises doivent envisager de mettre en œuvre un programme de gestion des risques tiers fondé sur les critères suivants :

Certification de sécurité obligatoire. Les fournisseurs de services TI peuvent obtenir diverses certifications qui prouvent que leurs réseaux et leurs mécanismes de sécurité sont à la hauteur. Citons par exemple les normes SOC 2 et ISO 27001.

Évaluation de sécurité indépendante. Les entreprises peuvent procéder à une évaluation de sécurité indépendante pour sécuriser l'accès des fournisseurs de services TI à leur réseau. Il est préférable d'éviter de laisser auxdits fournisseurs le soin de déterminer eux-mêmes comment accéder au réseau de l'entreprise cliente. Mieux vaut obtenir une seconde opinion.

Assurance contre les cyberrisques des fournisseurs tiers. Les fournisseurs de services TI qui souscrivent une police d'assurance cyberrisques auront les ressources nécessaires pour intervenir en cas d'incident comme une attaque par rançongiciel.

MESURES SIMPLES POUR RÉDUIRE LES RISQUES D'ATTAQUE PAR RANÇONGICIEL

Aucune solution miracle ne protège les entreprises à cent pour cent contre les rançongiciels. Pour se défendre, ces dernières doivent disposer d'un programme de cybersécurité global robuste, dont des mécanismes de base comme des pare-feu, une protection de bout en bout et des capacités de filtrage des courriers électroniques et du contenu Web et de gestion des correctifs.

Elles peuvent également prendre des mesures simples et peu coûteuses pour freiner les attaques par rançongiciel, dont les suivantes :

Formation des employés

Les attaques par rançongiciel sont souvent lancées par courriel. Pour les prévenir, les entreprises peuvent offrir à leurs employés les connaissances requises pour les détecter et les signaler. Travelers offre à des titulaires d'assurance cyberrisques la possibilité d'offrir les formations de sensibilisation à la cybersécurité de HCL à leurs employés, et ce, sans frais supplémentaires (sauf au Québec).

Désactivation des macros Microsoft Office

Les employés peuvent malencontreusement cliquer sur la pièce jointe d'un courriel malveillant et exécuter ainsi une « macro » Microsoft Office qui tentera d'installer un rançongiciel. Les macros sont généralement désactivées par défaut, mais les utilisateurs peuvent les « accepter » et en autoriser l'exécution. Mieux vaut donc désactiver toutes les macros Microsoft Office en vertu d'une politique de groupe si votre entreprise ou vos utilisateurs n'en ont pas besoin.

Protocole de connexion à distance (RDP) bloqué

Des attaques de rançongiciel peuvent être lancées au moyen du protocole de connexion à distance (RDP). Les entreprises qui n'ont pas besoin de ce protocole doivent en bloquer l'usage externe et, si possible, interne en reconfigurant simplement leurs pare-feux.

Au quatrième trimestre de 2019, près de 60 % de toutes les attaques par rançongiciel impliquaient le protocole de connexion à distance.[4]

Accès privilégiés sécurisés

Après avoir compromis un réseau, les criminels tentent d'obtenir les privilèges administratifs qui leur permettent d'accéder aux biens les plus précieux de l'entreprise victime. La plupart des entreprises peuvent renforcer la sécurité de leurs accès privilégiés à moindres frais en demandant aux utilisateurs privilégiés d'utiliser des mots de passe plus robustes et des comptes administratifs distincts, et en interdisant aux utilisateurs ordinaires d'avoir des privilèges administratifs locaux. L'authentification à facteurs multiples des accès privilégiés est une méthode encore plus efficace d'atténuation des attaques par rançongiciel.

Renseignements de source ouverte

Les entreprises peuvent utiliser des sources d'information gratuites ou peu coûteuses sur les menaces pour se tenir au courant des outils et des techniques utilisés par les cybercriminels et pour ainsi mieux adapter leurs mécanismes de défense.

Évaluation des capacités de sauvegarde et de rétablissement

La sauvegarde des données ne suffit plus. Les entreprises doivent désormais sauvegarder leurs ressources de réseau critiques comme les serveurs Active Directory ainsi que leurs logiciels exclusifs et leurs bases de données difficilement remplaçables. Ces sauvegardes doivent être stockées en lieu sûr de sorte que les cybercriminels ne puissent pas les chiffrer ou les supprimer. Enfin, il est essentiel que les entreprises testent leurs capacités de sauvegarde et de rétablissement au moins une fois par an pour en assurer la disponibilité au moment où elles en auront le plus besoin.

*Pour en savoir plus sur nos **capacités en matière de cybersécurité**, consultez le site **travelerscanada.ca***

[1]SonicWall, « 2020 Cyber Threat Report. »
[2]Coveware, « Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate. »
[3]Coveware
[4]Coveware, « Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate. »
Lectures supplémentaires : Accenture, « Managing Ransomware: Practical Steps to Avoid Future Attacks. »

TRAVELERS

travelerscanada.ca