JUILLET 2024

AFFAIRE MARQUANTE

Décision 249 en vertu de la LPRPS

INTRODUCTION

Malheureusement, les attaques par rançongiciel ne sont pas rares, surtout à notre époque où les technologies progressent rapidement. Des individus malveillants s'y livrent pour soutirer de l'argent et causer du tort à d'autres personnes. Comme ces types d'attaques se multiplient, les dépositaires de renseignements sur la santé devraient mettre en place de solides mesures préventives pour minimiser et prévenir les risques des attaques liées à la cybersécurité.

CONTEXTE

Après avoir décelé une activité inhabituelle dans ses systèmes en décembre 2022, une clinique d'imagerie médicale (la « clinique ») a établi qu'elle avait été victime d'une attaque par rançongiciel. Les responsables ont réagi en fermant immédiatement les serveurs et en faisant appel à un conseiller juridique et à une équipe d'experts en cybersécurité pour les aider à maîtriser la situation, à faire enquête et à prendre les mesures correctives qui s'imposaient.

Une semaine après l'incident, la clinique a informé le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) qu'elle avait été victime d'une attaque par rançongiciel. Elle a précisé que jusqu'à 550 000 dossiers de patients et 1 600 000 dossiers de cas avaient peut-être été touchés par l'attaque.

Les experts de la clinique ont déterminé que l'auteur de cette attaque (un groupe de pirates connu) avait probablement pénétré dans le système par l'intermédiaire d'un compte inactif, qui disposait d'importants privilèges d'administration. Le pirate a chiffré et exfiltré des fichiers des dossiers médicaux électroniques et des serveurs de partage de fichiers, supprimé les copies de sauvegarde et exigé le paiement d'une rançon. En l'occurrence, la clinique n'a pas été en mesure de rétablir ses systèmes à l'aide de copies de sauvegarde et a dû fermer temporairement ses portes.

La clinique a payé la rançon, après quoi elle a pu déchiffrer les données sur les serveurs touchés et récupérer tous les fichiers concernés. La clinique a informé le public de l'atteinte à la vie privée en ligne et au sein de ses établissements.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

La clinique a expliqué au CIPVP qu'elle avait mis en place des mesures de sécurité avant l'incident. Cependant, le niveau élevé d'activité pendant l'attaque a entraîné l'écrasement des journaux avant qu'ils ne puissent être examinés. La clinique n'a donc pas pu déterminer exactement comment cette intrusion était survenue ni quelles tactiques avaient été utilisées pour obtenir l'accès aux identifiants du compte.

Depuis cet incident, la clinique a pris des mesures correctives pour renforcer sa sécurité en instaurant plusieurs politiques et pratiques visant à empêcher que des situations semblables ne se reproduisent. Par exemple, la clinique a modifié sa politique de restriction des privilèges d'accès afin de limiter l'accès au domaine à deux membres du personnel administratif et de réduire l'accès des utilisateurs au minimum nécessaire pour l'exercice de leurs fonctions. La clinique a établi des exigences quant à la force et à la complexité des mots de passe, surveille et supprime les comptes inactifs et effectue des vérifications régulières pour s'assurer que tous les correctifs de sécurité ont été installés.

La clinique a également séparé ses réseaux et mis en place des pare-feu si nécessaire. En ce qui concerne les copies de sauvegarde, la clinique conserve désormais au moins une copie fiable hors ligne qui ne serait pas touchée en cas de nouvelle cyberattaque, afin que la clinique puisse reprendre ses activités. La clinique a amélioré ses mesures de détection et d'intervention. Elle télécharge désormais quotidiennement les journaux de son réseau privé virtuel et de son pare-feu et les conserve afin de pouvoir mieux enquêter sur de futurs cyberincidents grâce à ces journaux.

CONCLUSIONS

L'enquêteuse du CIPVP a établi que la clinique avait déployé des efforts suffisants pour déterminer l'ampleur de l'atteinte à la vie privée et donner un avis approprié. Elle a conclu que la clinique avait réagi de manière adéquate à cet incident, compte tenu notamment des mesures correctives qu'elle avait prises pour remédier à la situation. L'enquêteuse a également établi que la clinique avait donné un avis et mis en place des mesures correctives efficaces, et qu'il n'y avait donc pas lieu de procéder à un examen.

PRINCIPAUX CONSTATS

Cette affaire souligne pour les dépositaires de renseignements sur la santé l'importance de mettre en place des mesures de sécurité rigoureuses pour prévenir les cyberattaques, notamment :

(a) accorder un accès administratif privilégié à un nombre très limité d'utilisateurs

(b) réduire l'accès des utilisateurs au système au minimum nécessaire pour leurs fonctions et veiller à ce que cet accès soit supprimé lorsqu'un utilisateur quitte l'institution ou change de poste

(c) surveiller et supprimer les comptes inactifs

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

(d) exiger des mots de passe forts

(e) assurer une protection contre le virus et filtrer les pourriels

(f) munir le réseau de pare-feu et d'une connexion externe à un réseau privé virtuel

(g) instaurer l'authentification multifacteur

(h) vérifier régulièrement que les derniers correctifs de sécurité ont été installés

(i) fournir régulièrement au personnel une formation sur la cybersécurité

(j) tenir des journaux d'accès dotés d'une capacité suffisante, qui peuvent permettre de déceler rapidement les accès non autorisés aux systèmes et contribuer à déterminer la cause des incidents, le moment où ils se sont produits et comment ils ont été perpétrés

(k) effectuer des copies de sauvegarde fiables, dont au moins une est conservée hors ligne pour qu'elle demeure intacte en cas de cyberattaque, afin que le dépositaire de renseignements sur la santé soit en mesure de reprendre plus rapidement ses activités

Ce ne sont là que quelques mesures que les dépositaires de renseignements sur la santé peuvent prendre pour prévenir les cyberattaques et en atténuer les conséquences. Pour en savoir davantage sur les mesures préventives que peuvent prendre les dépositaires de renseignements sur la santé, consultez la feuille-info ***Se protéger contre les rançongiciels*** du CIPVP.

Lorsqu'une atteinte à la vie privée se produit, il est essentiel que le dépositaire de renseignements sur la santé prenne des mesures immédiates pour la maîtriser, notamment en mettant ses serveurs hors fonction et en faisant appel à un conseiller juridique et à une équipe d'experts en cybersécurité. Les dépositaires de renseignements sur la santé devraient également consulter le document d'orientation ***Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé*** du CIPVP pour ce qui concerne les mesures appropriées à prendre après une atteinte à la vie privée.

Prévenir une attaque par rançongiciel n'est pas une tâche facile. Cela demande du temps et des ressources. Toutefois, si des mesures de sécurité appropriées et solides sont mises en place au préalable, il est moins probable qu'un pirate parvienne à ses fins. Il est moins coûteux de prendre des mesures préventives que de payer une rançon ou de reconstituer un système compromis.