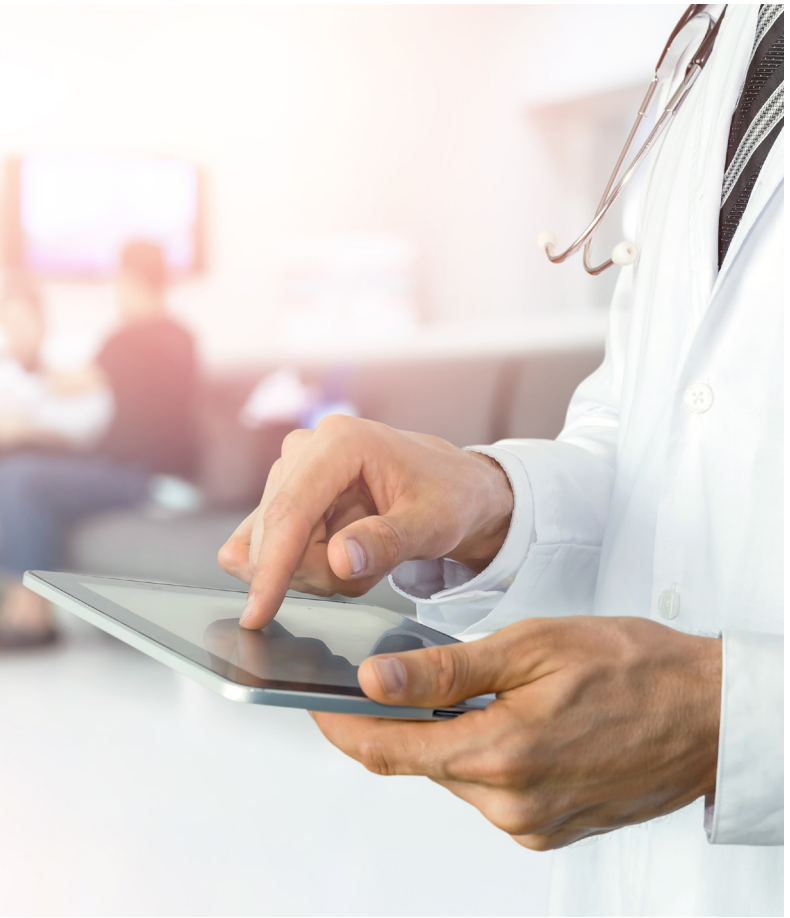
SCÉNARIO DE RÉCLAMATION

Au-delà de l'attaque

Un petit hôpital doit faire face à d'énormes perturbations opérationnelles

VICTOR



Étant donné que les fournisseurs de soins de santé détiennent généralement de grandes quantités d'informations très sensibles sur la santé de leurs patients, il est couramment considéré que leur principal risque cybernétique est la violation de données et les exigences de notification, les coûts des enquêtes, les amendes et les pénalités qui peuvent en résulter.

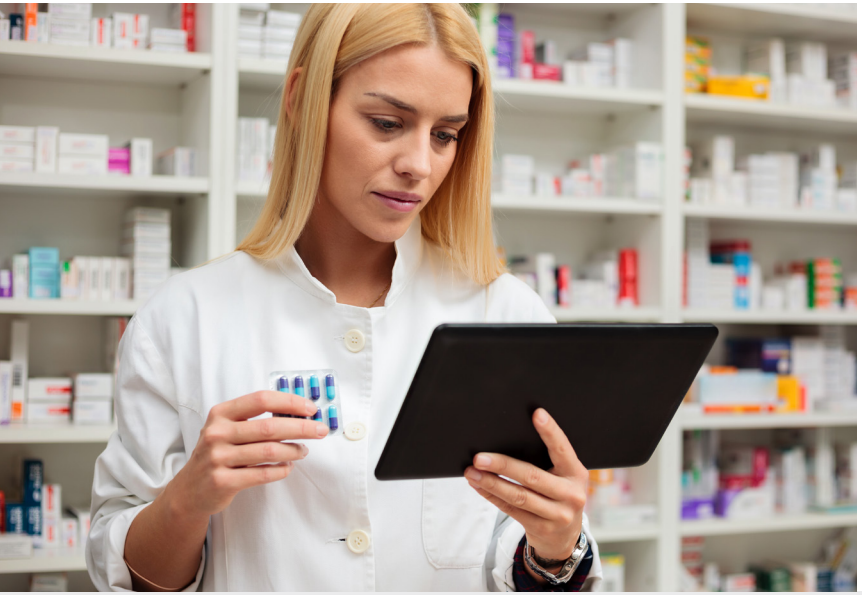
Mais les fournisseurs de soins de santé, comme toute entreprise, sont exposés à toute une gamme de risques cybernétiques, y compris les attaques de logiciels malveillants, qui peuvent avoir un impact dévastateur sur leurs opérations, notamment en ce qui concerne les dommages aux systèmes et les pertes d'exploitation.

Le saviez-vous?

Chaque jour, 350 000 nouveaux programmes malveillants sont découverts.

Source : AV-Test, IT Security Institute

Des logiciels malveillants à l'effondrement



Les logiciels malveillants sont des logiciels conçus spécifiquement pour endommager les réseaux informatiques, et des événements récents ont montré que les attaques de logiciels malveillants sont de plus en plus destructrices. Les motifs de ces attaques peuvent varier, allant de la tentative d'extorsion d'argent au fait d'infliger des dommages juste pour mal faire, mais dans tous les cas, l'impact sur l'organisation qui en est la victime peut être très perturbant et parfois catastrophique. En outre, les logiciels malveillants sont de plus en plus faciles à déployer avec l'augmentation constante des campagnes d'hameçonnage, qui ne sont qu'un moyen parmi d'autres de mener des attaques.

Un certain nombre d'organisations renommées ont été victimes d'attaques de logiciels malveillants ces dernières années. Par exemple, une entreprise d'emballage en plastique basée à Winnipeg a dû faire face à une perturbation importante de ses activités en raison d'une attaque de rançongiciel sophistiquée. Il lui a fallu deux semaines pour se rétablir complètement et reprendre ses activités normales.

En 2021, Terre-Neuve-et-Labrador a connu une autre cyberattaque qui a entraîné une perturbation généralisée des services de soins de santé dans toute la province. Cette attaque a eu de graves conséquences car elle a compromis les informations personnelles et les dossiers médicaux.

Cependant, les grandes entreprises ne sont pas les seules à être touchées par ce type d'attaques de logiciels malveillants. Des entités beaucoup plus petites peuvent également être affectées. L'une de ces victimes était un hôpital de taille moyenne aux États-Unis, qui pratique diverses interventions chirurgicales pour des patients recommandés par des médecins et qui gère un grand nombre d'admissions d'urgence.

C'est à la fin du mois d'août 2017 que l'hôpital a remarqué pour la première fois que quelque chose n'allait pas lorsque les employés sont arrivés au travail pour constater que tous les appareils et serveurs de l'hôpital ne fonctionnaient plus correctement. Cela signifiait que toutes les données électroniques que l'hôpital détenait sur ses patients étaient désormais inaccessibles. Le personnel de l'hôpital ne pouvait plus consulter les antécédents médicaux de ses patients, tels que les notes des médecins prises lors de visites précédentes, les allergies et les prescriptions de médicaments. Au lieu de pouvoir consulter les dossiers électroniques des patients comme ils le feraient normalement, les médecins et les infirmières devaient à nouveau interroger chaque patient sur ses antécédents médicaux. La surveillance électronique des patients n'était donc plus possible, et les machines utilisées au chevet des patients pour la distribution des médicaments étaient devenues inutilisables. L'hôpital a donc dû faire appel à une armée d'infirmières supplémentaires pour assurer un suivi efficace des patients.

Remise en service

Malgré tous les efforts de l'hôpital, ces procédures manuelles entraînaient des retards importants dans le service. En milieu d'après-midi, l'hôpital a été contraint de déclencher une Alerte rouge. L'Alerte rouge est un protocole d'État qui oblige le personnel ambulancier à informer les patients que, bien que l'hôpital concerné accepte encore des patients, les temps d'attente pour les procédures seront **nettement plus longs que d'habitude**. Le patient peut alors choisir de se rendre à l'hôpital concerné ou d'être emmené dans l'un des autres hôpitaux de la région. Avec l'Alerte rouge en place, le nombre de patients a commencé à diminuer.

Cette épidémie de logiciels malveillants destructeurs avait rendu inopérants environ 2 000 appareils et serveurs de l'hôpital, et la remise en service de ces systèmes était une tâche considérable. Le seul moyen de rétablir le fonctionnement normal de l'hôpital était **de nettoyer et de reconstruire tous les serveurs et appareils à partir de zéro**. Mais le nettoyage des appareils et des serveurs s'est avéré plus coûteux que le simple achat de pièces de rechange.

Une autre complication à laquelle l'hôpital a été confronté était liée à son système de dossiers médicaux électroniques. Comme la plupart des organisations de soins de santé, cet hôpital était connecté à un système de dossiers médicaux électroniques centralisé et hébergé, qui lui donnait accès aux dossiers et aux détails des patients et permettait l'échange d'informations avec d'autres établissements de soins de santé. Cependant, en raison de l'épidémie de logiciels malveillants sur son système, l'hôpital a été coupé par son fournisseur de services, qui a refusé de le reconnecter tant que son réseau n'aurait pas été déclaré totalement propre et exempt de logiciels malveillants par un expert indépendant. Dans l'intervalle, l'hôpital devait se connecter à un réseau en nuage distinct pour accéder aux données dont il avait besoin, ce qui représentait **un coût supplémentaire de 2 000 $ par jour**.

Ce n'est que fin octobre 2017 que l'hôpital a pu lever l'Alerte rouge, et il a fallu attendre début novembre pour que la normalité soit rétablie. Dans l'intervalle, l'assuré a encouru quelques 2,6 millions de dollars de coûts liés à des dommages au système, dont la majeure partie consistait à remplacer des disques durs, des serveurs, des ordinateurs portables, des ordinateurs, des imprimantes, des appareils de numérisation, des licences de logiciels et autres, et un autre 4,5 millions de dollars de pertes d'exploitation, principalement dues à la baisse des revenus des patients à la suite de l'Alerte rouge. Malheureusement pour l'assuré, la limite de garantie de la police n'était que de 5 millions de dollars.

Alors que de nombreuses polices d'assurance contre les cyber-risques excluent les coûts de remplacement des biens corporels et du matériel électronique, la police d'assurance contre les cyber-risques de l'hôpital souscrite auprès de Victor prévoit une couverture de ces éléments lorsque c'est le moyen le plus efficace de rendre l'assuré opérationnel à nouveau, ainsi qu'une couverture des pertes d'exploitation.

Choisir la bonne police d'assurance contre les cyber-risques

Les logiciels malveillants sont l'un des nombreux risques cybernétiques qui peuvent avoir un impact destructeur sur toute entreprise, grande ou petite. Si les organisations qui traitent d'importants volumes de données sensibles ou personnelles ont longtemps considéré leur risque cybernétique en termes d'atteinte à la protection des données, **toute entreprise dont le fonctionnement repose sur des systèmes informatiques peut être exposée à un risque substantie**l, notamment en ce qui concerne les dommages aux systèmes et les pertes d'exploitation.

Dans le présent cas, l'hôpital avait spécifiquement souscrit sa police d'assurance contre les cyber-risques en pensant à une atteinte à la protection des données et n'avait opté que pour une limite de garantie de 5 millions de dollars. Il avait calculé le nombre de personnes concernées par ses données et le coût probable de leur notification et de la gestion de toute enquête ou sanction ultérieure, mais il n'avait pas pris en compte **les énormes coûts liés à l'interruption des activités** que pourraient résulter d'un logiciel malveillant destructeur, ce qui le laissait terriblement exposé au moment où le désastre se produisait. L'assuré a subi cette énorme perte sans qu'un seul dossier de patient ait été violé.

Lorsqu'ils souscrivent une police d'assurance contre les cyber-risques, les assurés et leurs courtiers doivent s'assurer qu'ils **prennent en compte toute la gamme des risques propres et des risques de responsabilité** auxquels ils pourraient être confrontés et qu'ils choisissent une limite de garantie adéquate en conséquence.

Visitez assurancevictor.ca/cyber pour en apprendre davantage.