HSB BI&I

Munich RE

Cyber-protection résidentielle
Bulletin de perte

La Compagnie d'Inspection et d'Assurance Chaudière et Machinerie du Canada (BI&I)

390, rue Bay
Bureau 2000
Toronto (Ontario) M5H 2Y2
Tél. : (416) 363-5491
biico.com

Suivez-nous

Cyber-protection résidentielle

Les renseignements numériques et les systèmes informatiques des propriétaires peuvent être endommagés, exploités ou détruits par un virus ou un pirate informatique. Comme le nombre de services et d'appareils connectés utilisés desquels les propriétaires dépendent s'accroît chaque jour, ils sont davantage exposés aux cyber-criminels à la recherche de moyens de les frauder. Même avec un logiciel antivirus installé sur les ordinateurs, les propriétaires demeurent vulnérables aux attaques informatiques et de nouveaux virus pouvant contourner les défenses connues continuent d'émerger.

Les polices d'assurance des propriétaires occupants sur le marché ne couvrent pas les pertes causées par ces types de cyber-menaces.

Une telle couverture est désormais disponible pour les propriétaires et les locataires par le biais de la Cyber-protection résidentielle de BI&I, laquelle fournit une couverture contre les attaques sur les ordinateurs et les appareils domestiques connectés, ainsi que la fraude en ligne et la cyber-extorsion.

Cyber-attaque sur un ordinateur

Un clic insouciant sur un lien malveillant ou une pièce jointe dans un courriel peut causer des dommages considérables au système d'exploitation d'un ordinateur personnel.

Un individu a ouvert un fichier électronique joint à un courriel qui semblait provenir de UPS. Le fichier électronique a libéré un virus nuisible appelé Virus XP qui effectuait « sa tournée ». Le virus a corrompu les données et reconfiguré l'ordinateur. Afin de restaurer le système, la décision de « repartir à zéro » a été prise, ce qui nécessitait de reformater le disque dur, d'effacer tout son contenu et de réinstaller le système d'exploitation et tous les logiciels d'applications. Cette option a été rendue possible uniquement grâce à la disponibilité d'une copie de sauvegarde.

Cyber-attaque sur un appareil domestique connecté

Un propriétaire peut croire, à tort, qu'il est la seule personne capable d'accéder à ses appareils domestiques intelligents et de les contrôler.

Un soir, l'Internet d'un assuré ne fonctionnait pas. Après les tentatives habituelles, le propriétaire a contacté le fournisseur d'accès Internet. Ce dernier a expliqué qu'il n'y avait pas de panne connue dans la région, cependant il avait remarqué une activité étrange sur le compte. Quelqu'un avait réussi à accéder au routeur sans fil et à ajouter de nouveaux services au compte, y compris l'ajout d'une nouvelle ligne téléphonique et la connexion d'un thermostat intelligent et d'un système de sécurité, fournissant des renseignements supplémentaires pour ce pirate informatique. Afin de réinstaller les deux systèmes, l'assuré a finalement dû appeler et payer pour obtenir les services de techniciens, des fournisseurs d'Internet et de sécurité.

Cyber-extorsion

Les cyber-criminels peuvent exiger de l'argent sous la menace de supprimer les fichiers informatiques ou de voler les renseignements personnels d'un propriétaire.

Une demande de rançon a été reçue le mardi avant l'Action de grâce. Un message est apparu sur l'écran d'ordinateur de la propriétaire peu de temps après qu'elle ait découvert que tous ses fichiers avaient été verrouillés. « Vos fichiers sont cryptés », annonçait le message. « Pour obtenir la clé permettant de décrypter les fichiers, vous devez payer 1 000 $ US ». Si le paiement n'était pas reçu dans la semaine, le prix passerait à 2 000 $. La menace comprenait la destruction de sa clé de décryptage et toute possibilité d'accéder aux milliers de fichiers de son PC – toutes ses données – seraient perdues pour toujours. La propriétaire a acquitté la demande d'extorsion de 1 000 $ et a dû payer une firme de technologie de l'information pour enquêter sur la demande de rançons et s'assurer qu'aucun virus ne demeure dans son ordinateur.

Fraude en ligne

Les criminels continuent de trouver des moyens créatifs d'appâter les personnes peu méfiantes dans des stratagèmes frauduleux via Internet.

Un matin un propriétaire a reçu un courriel de son petit-fils Tommy qui avait des ennuis. Le courriel de Tommy indiquait qu'il avait été impliqué dans un accident de voiture la veille. Ce dernier faisait face à d'éventuelles accusations criminelles et il avait besoin d'argent pour les services d'un avocat. Dans un interval de 20 minutes, le propriétaire a reçu un second courriel. Celui-ci provenait d'un homme s'identifiant comme étant l'avocat de Tommy et fournissait un résumé de la situation d'un ton brusque, mais professionnel. Apparemment, la conductrice de l'autre voiture, une diplomate étrangère, était blessée. La diplomate avait convenu d'accepter 1 950 $ pour couvrir ses frais. Elle était prête à signer une quittance dès que le propriétaire aurait viré les fonds et fourni à l'avocat le numéro d'enregistrement du virement. Le propriétaire a appelé Tommy, mais il n'a pas répondu. Craignant pour son petit-fils, il a payé en espèces par le biais de MoneyGram et a transmis par courriel le numéro d'enregistrement à l'avocat. Le lendemain matin, le propriétaire a reçu un autre courriel provenant de l'avocat demandant plus d'argent, ce qui a semé le doute dans son esprit. Il a appelé son petit-fils à nouveau, pour découvrir que Tommy n'avait jamais été impliqué dans un accident.

Violation des données

La plupart des personnes ne réalisent pas qu'elles peuvent détenir des renseignements sensibles de tiers les rendant responsables de notifier les individus affectés si ces renseignements étaient perdus ou volés.

Une maman effectue régulièrement du bénévolat dans les écoles de ses enfants, aidant les enseignants à suivre les anniversaires des élèves et leurs numéros de compte-repas. Elle utilise une feuille de calcul sur sa tablette électronique personnelle. La tablette n'est pas sécurisée à l'aide d'un mot de passe et les données contenues dans la feuille de calcul ne sont pas cryptées. Lors d'une excursion, elle laisse la tablette dans l'autobus; celle ci n'a jamais été retrouvée. La perte de ces renseignements personnels est considérée comme une violation de données. Craignant que les familles de l'école ne soient victimes de vol d'identité, la femme a appelé son avocat qui lui a conseillé d'informer les familles affectées et de leur fournir des services d'alerte à la fraude et de gestion des cas.