Pourquoi les entreprises de services financiers sont-elles une cible importante ?

En tant que professionnel du secteur financier, vous disposez d'une grande quantité d'informations et de données sensibles sur vos clients. Les données personnelles identifiables (DPI) ont une valeur énorme pour les cybercriminels et leur accès fait de vous une cible pour les cyberattaques. Si vous n'êtes pas préparé ou si vous n'êtes pas suffisamment protégé, vous pouvez être vulnérable aux logiciels malveillants, aux rançongiciels, à l'hameçonnage, au vol d'informations d'identification et à bien d'autres choses encore, sans parler de l'effet que cela aurait sur votre réputation et, surtout, sur vos clients.

Les grandes comme les petites entreprises sont vulnérables

Le risque d'être la cible d'une cyberattaque ne concerne pas seulement les grandes entreprises. Bien que ces dernières entreposent plus de données, elles ont aussi beaucoup plus d'expérience et de ressources consacrées à l'amélioration de la cybersécurité et à la récupération après une cyberattaque.

En tant que professionnel d'une petite entreprise, vous vous concentrez sur la gestion de votre entreprise et le service aux clients. Cela vous laisse peu de temps pour vous tenir informé des dernières cybermenaces et pour mettre en place une stratégie de défense solide. Vous êtes donc plus vulnérable qu'une grande entreprise qui dispose de ressources dédiées et, en comparaison, une cible plus facile aux yeux des cybercriminels.

La conformité peut être compliquée, mais l'objectif est simple

Les exigences de conformité en matière de protection de la vie privée peuvent être compliquées, car elles sont souvent techniques et en constante évolution, mais les directives générales exigent que les DPI soient conservées de manière sûre et sécurisée. Il est de votre responsabilité de respecter les exigences de conformité et, ce faisant, vous protégerez votre propre entreprise.
« Disposer d'un système informatique sûr dans votre cabinet vous permettra de remplir 80 % de vos obligations en matière de législation sur la protection de la vie privée. » ERIC WACHTEL, directeur national de la conformité, IDC WIN.

Les violations de données doivent être signalées

Toute atteinte à la protection des données qui présente un risque réel de préjudice important pour une personne doit être signalée à la commission fédérale ou provinciale (selon la province de l'atteinte) et divulguée à la personne touchée, y compris (mais sans s'y limiter) la perte financière, le vol d'identité, les répercussions sur la cote de crédit, l'atteinte à la réputation ou

aux relations et la perte d'emploi, d'occasions d'affaires ou de possibilités professionnelles. Une telle violation oblige souvent le conseiller à payer pour que le ou les clients concernés soient inscrits à un service d'alerte de crédit pour une période de deux ans, au coût de 19,95 $ par mois et par personne. Multipliez ce montant par le nombre de clients avec lesquels vous travaillez et les dommages pourraient se chiffrer en milliers ou dizaines de milliers de dollars.

Comment atténuer les risques

La meilleure défense contre les cyberattaques est d'être conscient des risques et de prendre des mesures pour les prévenir. Il existe des changements que vous pouvez apporter dans votre propre entreprise pour améliorer la cybersécurité et réduire le risque d'être victime d'une cyberattaque.

Si vous n'en avez pas encore, il est important d'établir des politiques de cybersécurité et un plan de réponse aux incidents pour votre entreprise. L'élaboration de ces documents vous permettra d'examiner la manière dont votre entreprise traite déjà les données et de mettre en évidence vos éventuelles vulnérabilités. Dans les mois à venir, nous partagerons des informations et des conseils sur certaines mesures de sécurité clés que vous devriez inclure dans ces politiques, comme les directives relatives aux mots de passe forts et au traitement des données sensibles.

Partenariat avec IDC WIN

IDC WIN a choisi de s'associer à NPC pour vous proposer un programme de sécurité informatique visant à aider les conseillers à protéger leur entreprise et les informations sensibles qu'ils gèrent. NPC est spécialisée dans les solutions informatiques gérées et sécurisées, afin d'aider tous les professionnels à garder une longueur d'avance sur les cybermenaces émergentes.

Laissez NPC alléger la pression sur vous pour protéger les données des clients afin que vous puissiez vous concentrer sur le développement de votre entreprise. Le programme ICI comprend une offre spéciale pour vous aider à investir dans l'amélioration de votre posture de cybersécurité. Contactez Denis Goulet pour plus de détails dgoulet@npcdataguard.com .

Source: Rebecca Ungarino, "Cyberattacks are 300 times as likely to hit financial firms than other companies. A sweeping new report finds they're not prepared.", Business Insider, 20 June, 2019.

NPC DataGuard,
a division of Compugen Inc.
1-855-667-2642
info@npcdataguard.com
www.npcdataguard.com