ARSF
Autorité ontarienne de réglementation des services financiers

Information

Date d'entrée en vigueur : à déterminer
Identifiant : Nº. MB0048INF

Principes de préparation à la cybersécurité du Conseil canadien des autorités de réglementation des courtiers hypothécaires pour le secteur du courtage d'hypothèques

Objectif

La présente ligne directrice fournit des renseignements concernant :

- l'adoption par l'ARSF des principes de préparation à la cybersécurité du Conseil canadien des autorités de réglementation des courtiers hypothécaires (« directive de cybersécurité du CCARCH ») dans son cadre réglementaire.

- Le « protocole de surveillance des pratiques de l'industrie en matière de cybersécurité », qui est activé pour un engagement avec les titulaires de permis qui vivent un incident lié à la cybersécurité qui pourrait avoir un effet important sur les renseignements des clients.

La directive de cybersécurité du CCARCH a été élaborée pour aider à améliorer la préparation à la cybersécurité dans le secteur du courtage d'hypothèques par la création de pratiques de pointe suggérées pour prévenir les incidents de cybersécurité et y répondre de manière appropriée lorsqu'ils se produisent.

Ontario

Portée

La présente ligne directrice touche les personnes et les entités suivantes qui sont réglementées par l'ARSF :

- les agents en hypothèques;
- les courtiers hypothécaires;
- les maisons de courtage d'hypothèques;
- les administrateurs d'hypothèques.

Justification et contexte

Les cyberattaques représentent un risque important dans les secteurs réglementés par l'ARSF. Le flux d'informations entre les maisons de courtage d'hypothèques, les administrateurs, les prêteurs/investisseurs, les emprunteurs et les fournisseurs de services tiers est susceptible d'être perturbé ou compromis.

La cybersécurité est l'application de technologies, de processus et de contrôles pour protéger les infrastructures telles que les systèmes, les réseaux, les programmes, les appareils et les données. Elle vise à réduire la probabilité et l'impact des cyberattaques qui pourraient entraîner un accès non autorisé aux renseignements sensibles des clients et une perturbation des activités commerciales en raison de l'interférence avec les infrastructures critiques et les réseaux d'entreprise.

La directive en matière de cybersécurité du CCARCH, et l'adoption de cette directive par l'ARSF, vise à soutenir la préparation à la cybersécurité dans le secteur du courtage d'hypothèques en fournissant des pratiques exemplaires pour prévenir les cyberincidents et y répondre de manière appropriée lorsqu'ils se produisent. En tant qu'autorité de réglementation des pratiques de l'industrie, l'ARSF a pour objectif de protéger l'accès non autorisé aux renseignements sensibles des clients. Aux fins de la présente ligne directrice, les renseignements relatifs ayx clients désignent tous les renseignements relatifs aux consommateurs, y compris les emprunteurs, les prêteurs/investisseurs et les clients potentiels.

Mandat de l'ARSF

En supervisant et en réglementant le secteur du courtage d'hypothèques, l'ARSF vise à atteindre ses objectifs statutaires qui, aux fins de la présente ligne directrice, sont les suivants :

- contribuer à la confiance du public envers le secteur du courtage d'hypothèques.
- surveiller et évaluer les tendances dans le secteur du courtage d'hypothèques.
- coopérer et collaborer avec les autres organismes de réglementation, le cas échéant.
- protéger les droits et les intérêts des consommateurs.

Cadre juridique pour les renseignements personnels

Le cadre juridique canadien exige que les renseignements personnels soient protégés. En vertu de la Loi fédérale sur la protection des renseignements personnels et les documents électroniques et du projet de Loi fédérale sur la protection de la vie privée des consommateurs, toutes les entreprises, y compris les maisons de courtage et les administrateurs d'hypothèques, ont l'obligation de protéger les renseignements personnels précis des clients. Par exemple, les données personnelles recueillies doivent être conservées en toute sécurité et protégées contre la perte, l'accès non autorisé et le vol de données.

Code de conduite du CCARCH pour le secteur du courtage d'hypothèques

En vertu du principe 8 du Code de conduite du CCARCH pour le secteur du courtage d'hypothèques, « Les personnes et les entités réglementées doivent protéger les renseignements relatifs à leurs clients et doivent utiliser et divulguer ces renseignements uniquement aux fins pour lesquelles les clients ont donné leur consentement ou si la loi l'exige. »

Directive de cybersécurité du CCARCH

Pour aider les entités titulaires d'un permis de l'ARSF à s'acquitter de ces obligations et à gérer efficacement les risques liés à la cybersécurité, l'ARSF attend des entités qu'elles mettent en œuvre les « principes » identifiés dans la directive de cybersécurité du CCARCH. Les principes décrivent les résultats que les entités réglementées devraient atteindre pour assurer la préparation à la cybersécurité, sans prescrire la manière dont ils devraient être atteints. Cette approche fondée sur des principes permet aux entités réglementées d'atteindre les résultats d'une manière adaptée à la taille et à la structure de leurs activités.

La directive de cybersécurité du CCARCH inclut une liste de contrôle pour aider les entités à évaluer leur préparation à la cybersécurité.

Exigence en matière de formation continue

En vertu de l'article 9 du Règlement de l'Ontario 409/07 (Règl. de l'Ont. 409/07) pris en application de la Loi de 2006 sur les maisons de courtage d'hypothèques, les prêteurs hypothécaires et les administrateurs d'hypothèques, l'ARSF a le pouvoir d'établir des exigences en matière de formation continue (FC) pour les agents et les courtiers en hypothèques. Les agents et les courtiers qui souhaitent renouveler leur permis doivent satisfaire à l'exigence de formation continue approuvée par le directeur général de l'ARSF.

Les exigences de formation continue de l'ARSF comprennent de la formation et des sujets relatifs à la cybersécurité, au besoin. L'objectif de cette formation continue est de faire en sorte que chaque titulaire de permis comprenne comment reconnaître les menaces en matière de cybersécurité et prendre des mesures pour s'en protéger. Pour les maisons de courtage d'hypothèques et les administrateurs, l'ARSF souhaite soutenir l'industrie en veillant à ce que des processus soient en place pour reconnaître les risques liés à la cybersécurité, les surveiller et y répondre afin de contribuer à protéger les renseignements des clients.

Protocole de surveillance des pratiques de l'industrie de l'ARSF en matière de cybersécurité

Notification des incidents liés à la cybersécurité

Les maisons de courtage d'hypothèques et les administrateurs devraient informer l'ARSF en cas d'incident lié à la cybersécurité qui pourrait avoir un impact important sur les renseignements des clients, car l'ARSF veut s'assurer que :

- des mesures appropriées sont prises pour protéger les clients;
- l'organisme de réglementation possède des renseignements à jour pour répondre à toute question du public.
- les messages de l'organisme de réglementation et du titulaire de permis sont cohérents, afin d'éviter toute alarme indue.

L’organisme de réglementation devrait être informé dès que le titulaire de permis détermine qu’un incident lié à la cybersécurité pourrait avoir un impact important sur les clients. Voici quelques indicateurs qu’un incident lié à la cybersécurité pourrait avoir un impact important sur les clients :

- la violation de sécurité a touché un système ou une base de données qui stocke une grande quantité ou une proportion importante de renseignements sensibles sur les clients.

- dans le cours normal de ses activités, la maison de courtage ou l’administrateur d’hypothèques, transmettrait le problème à la haute direction responsable de la sécurité de l’information ou l’informerait.

- l’incident lié à la sécurité nécessite des mesures ou des ressources non habituelles de la part de la maison de courtage ou de l’administrateur d’hypothèques.

- l’incident lié à la sécurité a déclenché une demande d’indemnisation d’assurance.

- la violation est un incident répété et pourrait avoir un impact important sur une base cumulative.

Activation du protocole de surveillance des pratiques de l’industrie de l’ARSF en matière de cybersécurité

Lorsque l’ARSF prend connaissance d’un incident lié à la cybersécurité parce qu’il en est informé par l’entremise d’un titulaire de permis, de renseignements sur le marché, d’un tuyau ou d’une plainte, elle active son protocole de surveillance des pratiques de l’industrie en matière de cybersécurité.

Le protocole décrit l'engagement attendu de l'ARSF auprès du titulaire de permis[1] afin de surveiller les actions de l'entité lors de l'enquête et de la réponse à l'incident. Cet engagement est continu, jusqu'à ce que l'ARSF ait :

- une compréhension et une connaissance complètes de l'étendue de la violation potentielle des données et des renseignements auxquels il a été accédé.
- la confirmation que tout renseignement corrompu a été restauré, que la violation a été atténuée ou contenue, ou les deux.
- la confirmation que tous les systèmes sont revenus en ligne et sont complètement fonctionnels.
- la confirmation que tous les intervenants concernés, y compris les clients et les autorités compétentes en matière de protection de la vie privée, ont été informés, et que des mesures raisonnables ont été prises par le titulaire de permis pour limiter le préjudice potentiel causé aux clients.
- une compréhension et une connaissance complètes des mesures de protection qui ont été mises en place pour s'assurer que le titulaire de permis est protégé contre des violations futures similaires.

L'ARSF maintiendra la confidentialité des incidents signalés dans la mesure permise par la loi.

La réponse aux incidents se déroule généralement par phases, de façon semblable au schéma ci-dessous :

Phase 1 : Réception immédiate des renseignements du titulaire de permis sur ce qu'il sait de la nature et de l'étendue de l'incident lié à la cybersécurité, sur ce qu'il a fait pour se rétablir et réagir, et sur les mesures supplémentaires prévues.

[1] Si l'ARSF a besoin de renseignements supplémentaires concernant un incident, conformément à l'article 29 de la LMCHPHAH, elle a le pouvoir d'exiger des titulaires de permis qu'ils fournissent au directeur général les renseignements et les documents supplémentaires que le directeur général peut demander, et ce, de la manière et dans le délai que le directeur général spécifie.

Phase 2 : Au fur et à mesure que des renseignements plus complets sont disponibles, réception de mises à jour régulières de la part du titulaire de permis sur l'étendue ou l'impact de l'incident sur ses clients et ses services. Les renseignements demandés dépendent de la nature de l'incident. Par exemple, dans le cas d'une violation de données, l'ARSF cherchera à comprendre clairement la nature et l'étendue de la violation de données et les risques qu'elle présente pour les renseignements des clients.

Phase 3 : Réception par l'ARSF du plan du titulaire de permis visant à éviter tout incident semblable lié à la cybersécurité à l'avenir.

Le niveau et la fréquence de l'engagement de l'ARSF auprès d'un titulaire de permis reflètent la nature et l'impact de l'incident lié à la cybersécurité et tiennent compte des ressources dont le titulaire de permis a besoin pour répondre à l'incident.

Date d'entrée en vigueur et examen futur

La présente ligne directrice entre en vigueur le [à déterminer] et sera révisée au plus tard le [à déterminer].

À propos de la présente ligne directrice

Le présent document est conforme au Cadre de lignes directrices de l'ARSF. En tant que ligne directrice en matière d'information, il décrit le point de vue de l'ARSF sur certains sujets sans créer de nouvelles obligations en matière de conformité pour les personnes réglementées.

Références

- Principes de préparation à la cybersécurité du CCARCH
- Code de conduite du CCARCH