IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

AVIS DE L'OCRCVM

Avis relatif à la formation
Note d'orientation

Destinataires à l'interne :
Affaires juridiques et conformité
Audit interne
Comptabilité réglementaire
Crédit
Détail
Financement des sociétés
Formation
Haute direction
Inscription
Institutions
Opérations
Pupitre de négociation
Recherche
Technologie et cybersécurité

Personnes-ressources :
Suzanne Lasrado
Chef principale de la conformité des finances
et des opérations
416 943-5880
slasrado@iiroc.ca

Ryan Li
Directeur de la sécurité de l'information
416 943-5890
rli@iiroc.ca

20-0235
Le 9 novembre 2020

La cybersécurité et la fraude – Protéger les clients

Nous décrivons dans le présent avis les types de cyberattaques et de fraudes qui visent les clients d'une société, mais qui ne représentent pas nécessairement une attaque contre cette dernière. Il y est question des mesures que les sociétés et les conseillers peuvent prendre pour limiter la perte de renseignements sur les clients ou les actifs que ceux-ci détiennent auprès de

la société, et ce qu'il faut faire lorsque ces renseignements ou actifs ont été compromis ou volés. Nous y précisons également quand et comment déclarer de tels incidents à l'OCRCVM.

Aperçu

Dans les avis précédents, l'OCRCVM mettait l'accent sur ce que les sociétés et les conseillers devaient faire pour se protéger eux-mêmes et protéger leurs clients d'une attaque visant la société. Cependant, les clients peuvent également être victimes de fraude ou d'un vol d'identité à la suite d'attaques qui ne visaient pas la société. Il arrive souvent qu'un client dont le compte a été compromis ne sache pas que ses données d'accès ou ses renseignements personnels ont été volés.

Les cyberattaquants et les fraudeurs cherchent à nuire au client en utilisant des informations obtenues frauduleusement à son sujet pour effectuer des opérations non autorisées ou voler des renseignements ou des actifs dans son compte. Les sociétés et les conseillers doivent rester vigilants afin de prévenir les pertes touchant les clients et les dommages causés par ces attaques. Par conséquent, les sociétés doivent sérieusement penser à mettre en œuvre des mesures de contrôle pour tenter d'atténuer le plus possible l'incidence et le risque de perte pour les clients dont le compte a été compromis.

Types d'incidents et d'attaques

Voici comment les clients de certaines de nos sociétés membres dont le compte a été compromis ont été attaqués :

Piratage psychologique

Une personne malveillante peut convaincre un conseiller ou un employé de la société de lui faire part de renseignements sensibles sur le client, de transférer les fonds du client ou d'effectuer des opérations non autorisées dans le compte du client en se faisant passer pour ce dernier ou pour une personne autorisée à agir en son nom. Ces attaques peuvent être réalisées par l'entremise de plusieurs moyens de communication différents, notamment le courriel, le téléphone, les messages textes et les services de livraison par messager.

Ouvertures de comptes frauduleux et intrusion dans les comptes

Un pirate peut utiliser des renseignements personnels obtenus frauduleusement sur le client pour :

- créer un compte au nom du client auprès de la société, et même y déposer des fonds à partir de renseignements bancaires obtenus de manière frauduleuse afin d'effectuer des opérations non autorisées;

- pirater le compte actuel du client et y voler des actifs ou y effectuer des opérations non autorisées.

Les divisions de négociation en ligne et les sociétés offrant des comptes sans conseils doivent rester à l'affût de tels incidents. Compte tenu de l'augmentation des cyberattaques liées à la pandémie et de l'augmentation importante des ouvertures de comptes depuis le début de la pandémie, nous recommandons fortement aux sociétés qui offrent des comptes sans conseils de rester particulièrement vigilantes et prudentes à l'égard de ce genre d'incidents.

Bourrage d'identifiants

Il s'agit d'un type de cyberattaque où des identifiants de connexion volés sont utilisés pour obtenir un accès non autorisé aux comptes des clients par le biais de demandes automatisées de connexion aux applications en ligne de la société. Ces identifiants de connexion figurent généralement dans des listes de noms d'utilisateur et de mots de passe qui ont vraisemblablement été volés à la suite d'une atteinte à la sécurité des données survenue ailleurs. Comme de nombreuses personnes ont tendance à utiliser la même combinaison de nom d'utilisateur et de mot de passe sur différents sites Web et différentes applications, ces types d'attaques peuvent souvent être utilisés avec succès pour pirater le compte d'un client auprès de la société.

Contrôles de protection, d'identification et de détection recommandés

Les sociétés doivent prévoir des contrôles pour prévenir et repérer les attaques visant leurs clients, par exemple :

1) **Mettre en œuvre des contrôles, des politiques et des procédures**, qui, au minimum :
   - obligent la société à réaliser une vérification indépendante de l'identité du client, notamment lors de l'ouverture de comptes par voie électronique[1];
   - obligent le client à procéder à une vérification indépendante des demandes de renseignements sensibles à son sujet ou des ordres dans le cadre d'opérations inhabituelles ou importantes;
   - établissent des périodes de détention et exigent une approbation supplémentaire de la société et une vérification du client avant le transfert d'actifs qui dépassent certaines limites établies;
   - établissent des processus pour :

[1] Les politiques de la société doivent aussi assurer la conformité avec les lois et règlements sur le recyclage des produits de la criminalité qui régissent la vérification des pièces d'identité en l'absence de la personne.

- répondre rapidement aux plaintes, aux appels et aux demandes des clients concernant des activités inhabituelles sur leur compte, des intrusions dans leurs comptes et le détournement d'actifs;
- enquêter rapidement sur une intrusion soupçonnée, une activité non autorisée ou la perte d'actifs dans le compte d'un client afin de déterminer la cause fondamentale et l'étendue de l'attaque.

2) Mettre en place des **comptes en ligne avec de solides contrôles d'authentification** :
   - Instaurer l'authentification à plusieurs facteurs;
   - Établir des règles d'accès conditionnel et des tests captcha[2];
   - Exiger des mots de passe forts et des changements fréquents.

3) **Inciter les conseillers** à la prudence lorsqu'ils traitent les demandes des clients, comme suit :
   - faire preuve d'une vigilance accrue en traitant les demandes relatives au transfert d'actifs hors du compte;
   - se demander si la demande du client semble inhabituelle et la vérifier en conséquence à l'aide d'informations que seuls le conseiller et le client connaissent en se posant les questions suivantes :
     - S'agit-il s'une demande habituelle pour ce client?
     - La demande a-t-elle été faite par l'entremise d'un canal habituel et d'une manière normalement utilisée par le client pour communiquer avec la société?
     - La demande semble-t-elle suspecte d'une façon ou d'une autre?
   - connaître les protocoles d'intervention de la société en cas de demande inhabituelle d'un client ou si une intrusion de compte est soupçonnée.

4) **Surveiller les comportements inhabituels** pour atténuer les impacts d'éventuelles fraudes ou cyberattaques :
   - surveiller les alertes en temps réel et les examens de conformité après les opérations pour détecter tout écart anormal par rapport aux habitudes de négociation d'un client;
   - surveiller les variations anormales dans les demandes de connexion ou les activités;
   - bloquer l'accès au compte d'un client ou exiger une authentification supplémentaire si une adresse IP non reconnue est utilisée;
   - effectuer un suivi des listes d'adresses IP frauduleuses connues et bloquer l'accès aux systèmes de la société à partir de ces adresses.

[2] Un test captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) est une forme de test de Turing permettant de déterminer si la demande de connexion au compte en ligne provient d'une personne ou d'un ordinateur.

5) **Sensibiliser les clients** à la façon de se protéger contre la fraude en ligne et les informer sur ce qu'ils doivent faire s'ils soupçonnent que leur compte a été compromis :
    - en les avisant de ce qui suit :
        - ne pas divulguer leurs données de connexion ou renseignements personnels d'identification à qui que ce soit ou sur tout site Web ou application, à moins d'avoir vérifié personnellement et de façon indépendante la demande;
        - ne pas utiliser de réseaux sans fil publics;
        - configurer une authentification à plusieurs facteurs;
        - choisir des mots de passe forts;
        - aviser la société s'ils soupçonnent qu'ils ont été victimes d'un vol d'identité ou d'une fraude.
    - en leur fournissant les coordonnées des personnes-ressources et des instructions claires sur la façon d'informer la société s'ils remarquent des activités inhabituelles, ou soupçonnent une atteinte à leur compte, des opérations non autorisées ou un vol d'actifs;
    - en les renseignant sur leurs droits en vertu des différentes lois fédérales et provinciales et sur la manière de déposer une plainte auprès des autorités pertinentes.

6) **Fournir d'autres ressources ou services gratuits** aux clients :
    - webinaires et matériel de formation sur les menaces et les alertes en matière de cybersécurité;
    - téléchargement de logiciels antivirus, anti-espion et antimaliciels que les clients peuvent installer sur leur ordinateur pour accroître leur protection;
    - applications sécurisées pour créer et conserver les mots de passe.

Méthodes d'intervention et de rétablissement recommandées

Les sociétés doivent mettre en place des contrôles pour réagir aux attaques visant les clients, par exemple :

1) **Informer le ou les clients concernés** que leur compte a été compromis et leur recommander de faire ce qui suit :
    - modifier leurs données de connexion sur le site de la société et les autres sites Web;
    - demander un rapport au bureau de crédit.

2) **Prendre des mesures correctives pour protéger les comptes**, notamment en suspendant les comptes et en demandant aux clients de changer leurs mots de passe ou de créer de nouveaux comptes.

3) **Appeler l'établissement bancaire** pour faire interrompre le transfert des fonds, le cas échéant.

4) **Mener une enquête sur l'incident** pour déterminer la portée et l'étendue de l'attaque (même si elle semble isolée) afin de s'assurer que l'incident :
   - n'est pas le résultat d'une attaque visant la société;
   - ne s'est pas produit en raison d'un manquement de la société ou d'un employé de la société;
   - ne touche pas d'autres clients par effet de contagion ou n'entraîne pas de répercussions pour ces derniers.

5) **Signaler l'incident aux autorités**, aux commissaires à la protection de la vie privée, aux organismes de réglementation concernés et à l'OCRCVM. Pour en savoir plus sur la façon de signaler un incident à l'OCRCVM, se reporter à la section ci-dessous.

Signaler l'incident à l'OCRCVM

1) Si l'incident répond aux exigences de la Partie B.1.1 de la Règle 3100 des courtiers membres – ***Déclaration liée à la cybersécurité***, la société doit communiquer avec le chef de la conformité des finances et des opérations de l'OCRCVM dont elle relève et lui fournir les renseignements exigés.

2) **Toute enquête interne menée par la société ou toute plainte reçue de clients** en lien avec cet incident qui respecte les critères de la Règle 3100 de l'OCRCVM doit être signalée dans ComSet.

3) Si la société a des raisons de croire ou soupçonne qu'il y a eu une **activité de négociation non autorisée** dans le compte d'un client, nous lui demandons de signaler cet incident comme « intrusion dans les comptes » à l'OCRCVM. Les participants et les personnes ayant droit d'accès peuvent déposer un rapport relatif à l'obligation de veiller aux intérêts du client dans le portail des Services de l'OCRCVM.

4) Tout renseignement à propos **d'autres incidents** doit être communiqué à l'OCRCVM, à CyberIncidents@iiroc.ca.

Autres ressources

Vous trouverez des renseignements supplémentaires sur la gestion des cybermenaces ainsi que des ressources telles que des guides et des webinaires sur le site Web de l'OCRCVM, à la page Cybersécurité.