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

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

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

Avis de l'OCRCVM 20-0100
Le 14 mai 2020

La COVID-19 et la cybersécurité – Les services d'accès à distance

Le présent avis est destiné aux courtiers membres qui utilisent des services d'accès à distance (réseau privé virtuel [RPV], bureau virtuel, etc.) pour le télétravail.

Au cours des deux derniers mois, l'OCRCVM a publié un avis destiné aux sociétés et un avis destiné aux conseillers et aux autres employés des courtiers membres pour les informer du risque

accru de cyberattaques liées à la pandémie. Nous constatons que celles-ci continuent à évoluer et remarquons notamment une hausse des attaques visant à exploiter les vulnérabilités des services d'accès à distance.

Contexte

Les fournisseurs des services d'accès à distance ont signalé que des pirates informatiques sont en train de chercher activement des vulnérabilités potentielles dans les réseaux internes de différentes organisations. Ces pirates peuvent exploiter ces vulnérabilités pour tenter d'accéder à un réseau. S'ils y parviennent, ils resteront dissimulés et essayeront d'obtenir des privilèges d'accès additionnels pour entreprendre d'autres attaques, telles que des attaques par rançongiciel et le vol de données.

Que faire?

Les sociétés doivent continuer à faire preuve de vigilance et à appliquer des mesures de sécurité générales à l'égard de toutes leurs ressources informatiques, particulièrement les composantes dotées d'un accès externe telles que les services d'accès à distance.

Nous recommandons fortement que votre service des technologies de l'information ou votre fournisseur de services informatiques prenne les mesures suivantes :

1) **Apporter des correctifs à tous les systèmes** – s'assurer que des correctifs et des configurations de sécurité sont appliqués en temps opportun, selon les recommandations du fournisseur;

2) **Surveiller les environnements de réseau** – continuer à surveiller le réseau pour détecter toute activité anormale (attaque par force brute, activités de connexion ou activités de réseau anormales, etc.). Prendre des mesures immédiates en cas d'intrusion potentielle, par exemple en réinitialisant les mots de passe;

3) **Mettre en œuvre l'authentification multifacteur** – s'assurer que l'authentification multifacteur a été mise en œuvre et qu'elle est appliquée à tous les utilisateurs qui se connectent à partir d'un réseau externe;

4) **Installer un antivirus/antimaliciel et le mettre à jour régulièrement** – s'assurer qu'un antivirus/antimaliciel a été mis en place et qu'il contient les indicateurs de compromission les plus récents pour les serveurs, les terminaux et le réseau.

Autres ressources

Vous trouverez de l'information supplémentaire 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.