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 20-0133
Le 24 juin 2020

Cybersécurité – Services infonuagiques et interfaces de programmation d'applications

Le présent avis décrit certains contrôles de la technologie et de la cybersécurité liés à l'utilisation des services infonuagiques et des interfaces de programmation d'applications.

Les services infonuagiques et les interfaces de programmation d'applications sont de plus en plus ciblés, et leurs vulnérabilités, exploitées par les pirates informatiques. Le présent avis précise certaines pratiques recommandées que les sociétés peuvent adopter pour gérer ces risques. Vous devriez veiller à ce que votre fournisseur de services informatiques ou de services gérés examine et mette en œuvre des contrôles de la cybersécurité adaptés à votre société et à son environnement.

Services infonuagiques

Le recours aux services infonuagiques est en hausse. Ces derniers peuvent servir à accélérer les mises en œuvre, à faciliter l'accès à distance et à fournir des modèles sur demande pour les services informatiques. Selon sa mise en œuvre, la gestion d'un service infonuagique peut différer du déploiement traditionnel (dans les locaux) des serveurs, des applications et des services, et peut miser sur les contrôles d'accès au réseau et aux serveurs existants. Si vous êtes appelé à déployer et à gérer des environnements infonuagiques, envisagez de mettre en place les contrôles suivants :

1) **Mise en œuvre de méthodes d'authentification sûres** – Les environnements infonuagiques librement accessibles dans Internet peuvent exposer les données et les services de votre société à d'éventuelles attaques. Assurez-vous que des méthodes d'authentification fortes – authentification à facteurs multiples, accès conditionnel, etc. – ont été mises en place pour tous les utilisateurs et administrateurs afin que l'accès soit accordé au seul personnel autorisé.

2) **Compréhension claire des rôles et des responsabilités** – Certains contrôles de sécurité peuvent être assurés par le fournisseur de services infonuagiques alors que d'autres relèvent de la responsabilité de la société. En comprenant qui est responsable de quoi, vous vous assurez que tous les contrôles sont pris en compte.

3) **Création et suppression efficaces de l'accès des utilisateurs** – Les droits d'accès aux services infonuagiques des employés, sous-traitants et autres utilisateurs autorisés qui ont quitté la société doivent être révoqués séparément. Selon la configuration du compte de l'utilisateur, les droits d'accès de celui-ci aux services infonuagiques pourraient ne pas être automatiquement révoqués lorsque son compte Active Directory ou son compte de courriel est supprimé.

4) **Évaluation du fournisseur de services infonuagiques** – Avant d'engager un fournisseur de services infonuagiques, assurez-vous que votre société a effectué un contrôle diligent afin d'évaluer et d'approuver le fournisseur. Certains aspects à prendre en compte sont l'hébergement des données, les exigences de conformité, les processus de destruction des données, les antécédents du fournisseur, etc.

5) **Surveillance de l'environnement infonuagique** – Le nuage devient une extension de votre environnement informatique; il est donc impératif de suivre les événements liés à la sécurité dans le nuage, comme si la solution était déployée dans les locaux. Ce suivi permettra la détection des comportements inhabituels et atténuera ainsi les impacts d'éventuelles atteintes à la sécurité des données ou cyberattaques.

Interfaces de programmation d'applications (interfaces API)

Les sociétés peuvent rendre des données et des applications disponibles à l'externe au moyen de services et de protocoles d'application comme les interfaces API. Comme dans le cas des services infonuagiques, la sécurité des interfaces API assure la confidentialité de vos données et atténue le risque de mauvais usage des services d'application. Voici certains contrôles que votre société devrait envisager de mettre en place :

1) **Examen des flux de données et des processus** – Examinez le type de données exposées au moyen des services et protocoles d'application pour déterminer la classification et les contrôles à mettre en place à l'égard des interfaces API.

2) **Recours à de solides méthodes d'authentification et de chiffrement** – Plusieurs options d'authentification et de chiffrement sont offertes; le choix d'une méthode doit se faire en fonction du type de données auxquelles on peut accéder.

3) **Solutions permettant de détecter les attaques par force brute ou par déni de service distribué (DDoS)** – Les interfaces API sont conçues pour être accessibles de presque partout. Il faut donc s'attendre à des volumes d'opérations élevés et à de nombreuses tentatives de connexion. Le défi consiste à différencier les tentatives de connexion par force brute ou attaques DDoS et les connexions légitimes. Songez à mettre en place des solutions pour détecter les comportements inhabituels, notamment les tentatives de connexion à partir d'adresses IP malveillantes connues.

4) **Examen et modification de la conception des interfaces API** – Si le service ou le protocole d'application a été conçu ou configuré de façon non sécurisée, cela pourrait permettre à un pirate d'accéder à des données confidentielles ou d'interagir avec le service par des moyens indésirables. Les examens de la conception et les processus de gestion du changement avant le déploiement de ces services peuvent aider à détecter d'éventuelles vulnérabilités. De plus, en soumettant les applications à des tests et à des examens de sécurité réguliers, on peut éliminer toute faiblesse potentielle à la source.

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.