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

IIROC NOTICE

Education Notice

Please distribute internally to:
Corporate Finance
Credit
Institutional
Internal Audit
Legal and Compliance
Operations
Registration
Regulatory Accounting
Research
Retail
Senior Management
Trading Desk
Training

Contact:
Suzanne Lasrado
Senior Manager, Financial & Operations Compliance
416-943-5880
slasrado@iiroc.ca

Ryan Li
Director, Information Security
416-943-5890
rli@iiroc.ca

IIROC Notice 20-0133
June 24, 2020

Cybersecurity – Cloud Services and Application Programming Interfaces

This Notice outlines some technology and cybersecurity controls related to the use of cloud services and application interfaces.

Cloud services and application interfaces are being increasingly targeted and their vulnerabilities exploited by cyber attackers. This Notice identifies some recommended practices that firms can

consider to manage these risks. You should ensure that your IT or managed services provider reviews and implements cybersecurity controls applicable to your firm and environment.

Cloud services

The use of cloud services is increasing. Cloud services can help with providing quicker implementations, remote access capabilities, and on-demand models for computing services. Depending on the implementation, the management of a cloud service may differ from the traditional on-premises deployment of servers, applications, and services, which can leverage existing network and server controls. When deploying and managing cloud environments, consider the following controls:

1) **Implement secure authentication methods** – cloud environments available over the open Internet may expose your organization's data and services to potential attackers. Ensure strong authentication methods – like multi-factor authentication, conditional access rules, etc. – are in place for all users and administrators to ensure that only authorized personnel have access.

2) **Understand clear roles and responsibilities** – some security controls may be covered by the cloud services provider while others are the responsibility of the firm. Understanding who is responsible for what ensures that all controls are accounted for.

3) **Ensure an effective user onboarding and off boarding process** – accounts of departed employees, contractors or other authorized users must be separately removed from cloud services access. Depending on the setup, user accounts may not be automatically removed for cloud access when a user's Active Directory or email account is removed.

4) **Assess the cloud service provider** – prior to engaging a cloud provider, ensure your firm has conducted due diligence to assess and approve the cloud services provider. Some areas to consider include data residency, compliance requirements, data destruction processes, vendor history, etc.

5) **Monitor the cloud environment** – as the cloud becomes an extension of your IT environment, it is imperative that capabilities and processes are in place to also monitor for security events in the cloud as if the solution was deployed on-premises. Such monitoring will enable the detection of anomalous behaviour to mitigate the impacts of a potential data breach or cyber-attack.

Application Programming Interfaces (APIs)

Firms can make data and applications available outside of the organization through the use of application services and protocols like APIs. As with cloud services, security of APIs ensures the confidentiality of your data and mitigates misuse of application services. The following highlights some controls your firm should consider:

1) **Review data flows and processes** – review the type of data exposed through application services and protocols to determine the classification and the controls to put in place over such APIs.

2) **Use strong authentication and encryption methods** – there are a number of authentication and encryption options available based on the type of data that can be accessed.

3) **Consider solutions to detect brute force and distributed denial of service (DDoS) attacks** – APIs are designed such that they can potentially be accessed from almost anywhere. This means that high volumes of transaction or connection attempts are to be expected. The challenge is in differentiating between brute force connection attempts or DDoS attacks, and legitimate connection attempts. Consider solutions to detect for such anomalous behaviour including connection attempts from known malicious IP addresses.

4) **Review API designs and changes**– if the application service or protocol is designed or configured in an unsecure manner, it may allow an attacker to access confidential data or interact with the service through unintended means. Design reviews and change management processes prior to the deployment of such services can help to identify any vulnerabilities. Furthermore, regular security testing and review of applications can root out any potential weaknesses.

Other resources

Further information and resources on managing cybersecurity threats, including guides and webinars, are available on IIROC's cybersecurity site.