SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

SFC
證監會

Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading

Table of contents

Introduction		**1**
1.	**Protection of clients' internet trading accounts**	**2**
2.	**Infrastructure security management**	**3**
3.	**Cybersecurity management and supervision**	**5**

Introduction

1. These Guidelines are published by the Securities and Futures Commission (SFC) under section 399 of the Securities and Futures Ordinance (SFO) and set out the baseline requirements to reduce or mitigate hacking risks associated with internet trading.

2. These Guidelines should be read in conjunction with, among other provisions, paragraphs 18.4 to 18.7 of and paragraphs 1.1, 1.2.2 to 1.2.8, 1.3 and 2.1 of Schedule 7 to the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct). For the purposes of these Guidelines, "internet trading" has the same meaning as in Paragraph 18.2(f) of the Code of Conduct, being "an arrangement where order instructions are sent to a licensed or registered person through its internet-based trading facility".

3. These Guidelines apply to persons which are engaged in internet trading and are licensed by, or registered with, the SFC for:

    - Type 1 regulated activity (dealing in securities);
    - Type 2 regulated activity (dealing in futures contracts);
    - Type 3 regulated activity (leveraged foreign exchange trading). For the avoidance of doubt, these Guidelines shall only apply to leveraged foreign exchange traders licensed by the SFC; and/or
    - Type 9 regulated activity (asset management) to the extent that they distribute funds under their management through their internet-based trading facilities.

4. These Guidelines do not have the force of law and should not be interpreted in any manner which would override the provisions of any applicable law, codes or other regulatory requirements. However, a failure to follow the spirit of these Guidelines may reflect adversely on the person's fitness and properness.

5. The controls and measures specified in these Guidelines can only reduce or mitigate hacking risks associated with internet trading, but cannot eliminate them. It must be emphasised that these are the minimum standards expected of licensed or registered persons and are not meant to be exhaustive. Licensed or registered persons are expected to implement adequate and effective measures which are commensurate with their structure, business operations and needs.

1. Protection of clients' internet trading accounts

1.1. Two-factor authentication[1]

A licensed or registered person should implement two-factor authentication for login to clients' internet trading accounts.

A licensed or registered person should assess and implement a two-factor authentication solution which is commensurate with its business model.

1.2. Implement monitoring and surveillance mechanisms

A licensed or registered person should implement an effective monitoring and surveillance mechanism to detect unauthorised access to clients' internet trading accounts.

1.3. Prompt notification to clients

A licensed or registered person should notify clients (eg, via email, short message service (SMS) or other push notifications) promptly after certain client activities have taken place in their internet trading accounts. These activities should at least include:

(a) System login;

(b) Password reset;

(c) Trade execution;

(d) Fund transfer to third party accounts unless these have been registered with the licensed or registered person for fund transfer purposes prior to the transfer; and

(e) Changes to client and account-related information.

The channel of notification to clients should be different from the one used for system login (as outlined in paragraph 1.1).

Clients may choose to opt out from "trade execution" notifications only. Under such circumstances, adequate risk disclosures should be provided by the licensed or registered person to the client and an acknowledgement should be executed by the client confirming that the client understands the risks involved in doing so.

1.4. Data encryption

A licensed or registered person should use a strong encryption algorithm to:

(a) encrypt sensitive information such as client login credentials (ie, user ID and password) and trade data during transmission between internal networks and client devices; and

(b) protect client login passwords stored in its internet trading system.

[1] Two-factor authentica-tion refers to an authentication mechanism which utilises any two of the following factors: what a client knows, what a client has, and who a client is.

1.5. Protection of client login passwords

A licensed or registered person should establish and implement effective policies and procedures to ensure that a client login password is generated and delivered to a client in a secure manner during the account activation and password reset processes. A client login password should be randomly generated by the system and sent to a client through a channel of communication which is free from human intervention and from tampering by staff of the licensed or registered person.

In a situation where a client login password is not randomly generated by the system, the licensed or registered person should implement adequate compensating security controls such as compulsory change of password upon the first login after client account activation.

1.6. Stringent password policies and session timeout controls

A licensed or registered person should set up stringent password policies and session timeout controls in its internet trading system, which include:

(a) Minimum password length;

(b) Periodic reminders for those clients who have not changed their passwords for a long period;

(c) Minimum password complexity (ie, alphanumeric) and history;

(d) Appropriate controls on invalid login attempts; and

(e) Session timeout after a period of inactivity.

2. Infrastructure security management

2.1. Deploy a secure network infrastructure

A licensed or registered person should deploy a secure network infrastructure through proper network segmentation, ie, a Demilitarised Zone (DMZ) with multi-tiered firewalls, to protect critical systems (eg, internet trading system and settlement system) and client data against cyber-attacks.

2.2. User access management

A licensed or registered person should have policies and procedures in place to ensure that system access or the use of the systems are granted to users on a need-to-have basis. In addition, a licensed or registered person should review, at least on a yearly basis, the user access list of critical systems (eg, internet trading systems and settlement systems) and databases (eg, client data) to ensure that access to or use of the systems remain restricted to persons approved to use them on a need-to-have basis.

2.3. Security controls over remote connection

A licensed or registered person should grant remote access to its internal network on a need-to-have basis and implement security controls over such access.

2.4. Patch management

A licensed or registered person should monitor and evaluate security patches or hotfixes released by software provider(s) on a timely basis and, subject to an evaluation of the impact, conduct testing as soon as practicable and implement the security patches or hotfixes within one month following the completion of testing.

2.5. End-point protection

A licensed or registered person should implement and update anti-virus and anti-malware solutions (including the corresponding definition and signature files) on a timely basis to detect malicious applications and malware on critical system servers and workstations.

2.6. Unauthorised installation of hardware and software

A licensed or registered person should implement security controls to prevent unauthorised installation of hardware and software.

2.7. Physical security

A licensed or registered person should establish physical security policies and procedures to protect critical system components (eg, system servers and network devices) in a secure environment and to prevent unauthorised physical access to the facilities hosting the internet trading system as well as the critical system components.

2.8. System and data backup

A licensed or registered person should back up business records, client and transaction databases, servers and supporting documentation in an off-line medium on at least a daily basis.

A licensed or registered person should also adopt an appropriate recovery method to enable successful roll-back of major system changes.

2.9. Contingency planning for cybersecurity scenarios

In order to ensure that appropriate contingency procedures can be effectively executed when cybersecurity situations occur, a licensed or registered person should make all reasonable efforts to cover possible cyber-attack scenarios such as distributed denial-of-service (DDoS) attacks[2] and total loss of business records and client data resulting from cyber-attacks (eg, ransomware) in the contingency plan and crisis management procedures.

2.10. Third-party service providers

If a licensed or registered person has any arrangement to outsource any activities associated with its internet trading to a third-party service provider, it should enter into a formal service-level agreement with the service provider which specifies the terms of service and the responsibilities of the provider. In particular, a licensed or registered

[2] In a DDoS attack, multiple compromised computer systems attack a server, website or other network resource, and cause a denial of service for its users.

person should ensure that the services provided by the third-party service provider enable the licensed or registered person to comply with the relevant requirements set out in, among other provisions, Paragraph 18 and Schedule 7 to the Code of Conduct and these guidelines. Service level agreements should be regularly reviewed and revised, where appropriate, to reflect any changes to the outsourcing arrangements or regulatory developments. Wherever possible, such agreements should provide sufficient levels of maintenance and technical assistance with quantitative details.

3. Cybersecurity management and supervision

3.1. Roles and responsibilities of cybersecurity management

The responsible officer(s) or executive officer(s) responsible for the overall management and supervision of the internet trading system should define a cybersecurity risk management framework (including but not limited to policies and procedures), and set out key roles and responsibilities. These responsibilities include:

(a) Reviewing and approving cybersecurity risk management policies and procedures;

(b) Reviewing and approving the budget and spending on resources for cybersecurity risk management;

(c) Arranging to conduct a self-assessment of the overall cybersecurity risk management framework on a regular basis;

(d) Reviewing significant issues escalated from cybersecurity incident reporting;

(e) Reviewing major findings identified from internal and external audits and cybersecurity reviews; endorsing and monitoring the completion of remedial actions;

(f) Monitoring and assessing the latest cybersecurity threats and attacks;

(g) Reviewing and approving the contingency plan, which covers cybersecurity scenarios and corresponding contingency strategies, developed for the internet trading system; and

(h) Where applicable, reviewing and approving the service level agreement and contract with a third-party service provider relating to internet trading.

These responsibilities can be delegated, in writing, to a designated committee or operational unit, however overall accountability remains with the responsible officer(s) or executive officer(s).

3.2. Cybersecurity incident reporting

A licensed or registered person should establish written policies and procedures specifying the manner in which a suspected or actual cybersecurity incident should be escalated and reported internally (eg, to the responsible officer(s) or executive officer(s) in charge of internet trading) and externally (eg, to clients, the SFC and other enforcement bodies, where appropriate).

3.3. Cybersecurity awareness training for internal system users

A licensed or registered person should provide adequate cybersecurity awareness training to all internal system users[3] at least on a yearly basis. When designing the content of the training programme, the licensed or registered person should take into account the type and level of cybersecurity risks it faces.

3.4. Cybersecurity alert and reminder to clients

A licensed or registered person should take all reasonable steps to remind clients about and alert them to cybersecurity risks and recommended preventive and protection measures when using the internet trading system, such as that login credentials should be properly safeguarded and cannot be shared.

[3] Internal system users refers to any permanent and contract staff who have access to the internal network and systems of a licensed or registered person.