FINCSIRT

(Financial Sector Computer Security Incident Response Team)

Member Incident Identification and Reporting Guidelines

Introduction

This document is presented with a set of example incidents which the members are requested to notify FINCSIRT as and when the incident is taken in place. FINCSIRT will assist you as the first responder to the incident in taking proactive and reactive measures and at the same time alerting all the members of potential threats to the sector based on the criticality of the threat.

Members are requested to not to limit their selves to the following incidents and these incidents are examples to provide you better clearance to what incidents to alert FINCSIRT. Further, please make sure FINCISRT is added as a first responder to the company incident response policy as it facilitates the information flow more feasible.

Information security incident

An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible use policy.

Following is a set of example incidents that should be reported to FINCSIRT.

Examples of information security incidents

1. **Computer system intrusion, suspected or actual breaches, compromises or other unauthorized access to information systems, data, applications, or accounts**

    - Unauthorized computer system intrusion is when someone gains access to a website, program, server, service, or other system using someone else's account or any other methods.
        - Possible detection methods
            - Using FINCSIRT ISOC File Integrity Monitoring system alert tagged
                - "integrity checksum changed"
            - Using FINCSIRT ISOC LAS system alerts tagged
                - "Unknown user or bad password"
                - "Multiple authentication failures followed by a success"
                - "First time this user logged in this system"
                - "Listened ports status changed"
                - or other variations of alerts
            - Using web application firewall alerts.
            - Using IDS/IPS alerts.
            - Regular audit of access control lists versus the current active employment lists from HR.
            - Using any other log monitoring system alerts.

        - Requirement for FINCSIRT reporting – **Reporting is required**

2. **Unauthorized or inappropriate disclosure of sensitive institutional data**

    - Unauthorized or inappropriate disclosure of sensitive data is when intentionally or unintentionally a person from inside or outside discloses any highly-classified information that is sensitive to organizational business continuity or the reputation. these incidents are extremely hard to detect.
        - Possible detection methods
            - Through proper data access audits.
            - Proper security access controls.
            - Continue monitoring of media and internet dumps.
            - Through Data Leakage Prevention (DLP) system alerts.
            - Continue monitoring of unusual network usage (high uploads).

        - Requirement for FINCSIRT reporting – **Reporting is required**

3. **Unauthorized changes to computers or software**

    - A most common incident that occurs in various methods. This can be done by internal staff or an external party. While not in a malicious intent, a system change that done by an internal engineer that does not follow proper change request procedures also categorized in to this section.
        - Possible detection methods
            - Using FINCSIRT ISOC File Integrity/Registry Monitoring system alert tagged
                - "integrity checksum changed"
            - Through Configuration management system logs
            - Through File/System integrity verifications
            - Through system audits

        - Requirement for FINCSIRT reporting – **Reporting is required**

4. **Loss or theft of computer equipment or other data storage devices and media**

    - Loss or theft of data storage equipment (e.g.: laptop, USB drive, personally owned device used for office work) is considered as a high-risk incident that should be reported to proper channels including FINCSIRT/Police immediately. precautions should be made to reduce this risk such as physical security and mandatory data encryption.
        - Possible detection methods
            - Through periodic inventory audits on critical storage
            - Using surveillance cameras

        - Requirement for FINCSIRT reporting – **Reporting is required**

5. **Denial of service attack (DOS /DDOS) or an attack that prevents or impairs the authorized use of networks, systems, or applications**

    - The Denial of Service (DoS / DDoS) attack is focused on making a resource (website, application, server) unavailable for the purpose it was designed. If a service receives a very large number of requests, it may disrupt the service

availability for the legitimate users. While detection of an event is easy, determining whether it's an attack is extremely hard as distinguishing legitimate traffic from malicious traffic is hard.

- Possible detection methods
    - Using FINCSIRT ISOC OMS system alerts on service outages
    - Using FINCSIRT ISOC LAS system alerts tagged "Excessive number of events"
    - Using web application Firewall alert
    - Using IDS/IPS alert
    - Customer complaints
    - Using any other log monitoring system alert
    - Unexpected network slowness

- Requirement for FINCSIRT reporting – **Reporting is required**

6. Unauthorized Electronic Monitoring, Probe/Scan

- While authorized monitoring is always encouraged, unauthorized monitoring can mostly relate to active reconnaissance where an attacker looks for private information on the victim's systems. Even though we will not be able to stop the large number of reconnaissance's happening across globe, identifying attackers or Command-and-Control servers across globe that affects Sri Lankan Financial Sector is extremely important.

- Possible detection methods
    - Using FINCSIRT ISOC system alerts.
    - Using web application Firewall alerts.
    - Using IDS/IPS alerts.
    - Using any other log monitoring system alerts.

- Requirement for FINCSIRT reporting – **Reporting is required**

7. Misuse of Systems (internal or external)

- This includes various misuses among information systems that are not properly authorized and not accordance with the organizational policies.

- Possible detection methods
    - Through audit findings
    - Proper network monitoring
    - Surveillance systems
- Requirement for FINCSIRT reporting –
    - **For Internal: Reporting is optional**
    - **For External: Reporting is required**

8. Malicious Code (e.g. Virus, Worm)

- As one of most common incidents happening around the sector, it's extremely important to have malicious code detection techniques such as Virus Guards properly deployed throughout the organization.

- Possible detection methods
  - Using virus guard alerts.
  - Unusual behavior in IT systems
- Requirement for FINCSIRT reporting –
  - **General Virus guards alerts are not required to report**
  - **Reporting successful attacks or unusual behavior is required**

9. Email based Intrusions

- Email based attacks such as Phishing, Falsifying data, data breach, ransomware should be immediately reported as its' important to contain the attack while it is on the way. These are a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels. Typically, a victim receives a message that appears to have been sent by a known contact or organization.

  - Possible detection methods
    - Using email monitoring systems.
    - Reported by users
  - Requirement for FINCSIRT reporting – **Reporting is required**

10. Intrusion/Hack

- This includes various attacks or attack attempts such as Cross Site Scripting attack (XSS), Injection type attacks such as SQL injections, Password cracking attacks etc. These are extremely high priority attacks that should be informed to FINCSIRT as quickly as possible.

  - Possible detection methods
    - Using FINCSIRT ISOC system alert tagged "SQL injection"
    - Using FINCSIRT ISOC system alert tagged "Brute force"
    - Using FINCSIRT ISOC system alert tagged "Cross-Site Scripting"
    - Using FINCSIRT ISOC high priority system alerts
    - Using web application firewall alert
    - Using IDS/IPS alert
    - Using any other monitoring system alert
  - Requirement for FINCSIRT reporting – **Reporting is required**

11. ATM/Card related incidents

- Any kind of unusual behavior, breaches or skimming attempts on ATM/Card networks are always a high priority incident that should be reported to FINCSIRT immediately.

  - Possible detection methods
    - Surveillance systems
    - ATM monitoring systems alerts
    - Card center/Customer reported incidents
    - Unusual behavior detection
  - Requirement for FINCSIRT reporting – **Reporting is required**

12. **Other incidents**
    - External/Internal threats (espionage)
    - Extortion based on Information Systems
    - External/Internal Audit Findings related to any information security breach
        - Requirement for FINCSIRT reporting – **Reporting is required**

While attempting to include most of the common incidents, there are vast number of incidents that can be reported to FINCSIRT that will be beneficial for your organization and Sri Lankan Financial Sector. If you are in any doubt, please do contact us via following methods, so that we can assist you in determining, identifying and resolution of your information Security related incidents.

Hotline (24*7) - (+94 (0)11 256 6655)

Manager: manager@fincsirt.lk - (+94 (0)76 546 5830)

Asst. Manager: (+94 (0)76 527 7856)