INCIDENT RESPONSE METHODOLOGY

IRM #12
INSIDER ABUSE

Guidelines to handle and respond to internal information disclosed intentionally

IRM Author: CERT SG
Contributor: CERT aDvens
IRM version: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

C'EST VOUS L'AVENIR

SOCIETE GENERALE

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.

WHO SHOULD USE IRM SHEETS?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

→ IRM CERT aDvens (French version): https://github.com/cert-advens/IRM

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

IRM provides detailed information for each step of the incident response process. The steps come from NIST Computer Security Incident Handling Guide.

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

Contacts

- Make sure to have contact points in your public relation team, human resources team and legal department
- Centralize logging for access controls
- Make sure to have a global authorization and clearance process. This process must specially take care of the removal of privileges on former jobs
- Provide strong authentication accordingly to the risk of the business application
- Prepare internal and external communication strategy
- Prepare a Data Loss Prevention (DLP) process with GDPR and risk team

Be prepared to notify implicated providers and law enforcement services and regulators if required during an incident (cell crisis management).

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

Technical identification*

- Alerts from a SIEM or correlation tools:
  - Malicious behavior can have been detected with the correlation of several abnormal events.

- Alerts from an IDS/IPS detecting an intrusion:
  - In case the insider tried to hack the system, an Intrusion Detection System (or Intrusion Prevention System) can be able to trigger an alert.

- Alerts from DLP controls and services:
  - Tools and processes to detect and prevent data breaches and data exfiltration.

- Alerts from physical access controls

Human identification

- Management:
  - The manager of the insider might be the first to notice the suspected behavior.

- Control, risk, compliance:
  - These teams have their own systems to detect operational anomalies and they can also trigger alerts if something abnormal is detected.

- Colleagues:
  - Insider's colleagues are maybe the most valuable notification channel because they know perfectly the tasks, the process and the impacts on their duty jobs. They can guess easily what is happening.

- External parties:
  - External partners or structure can also have their own detection capabilities. If operations have been falsified internally, these external entities can bring a real enlightenment.

**For more details, check the Windows and Linux intrusion IRM-2 and IRM-3*

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

Don't do anything without a written request from the concerned CISO/DPO/person in charge. Based on your legal team advisory, a written permission from the concerned user might also be handy.

1. Involve people

Experts should be informed about the incident so that they can help to assist on it. This includes HR management, legal management, DLP team, PR management and business management of the suspected insider.

2. Meeting

An HR manager should meet the suspected insider to explain him/her what has been found and what will happen. Support can be required from legal, technical and management people.

3. Privileges lowering

If the suspected insider is allowed to stay at work until the end of the investigation, provide him/her a computer with minimum authorizations.

4. Authorization freeze

Suspend access and authorizations of the suspected insider. This must include application clearance. This can also include system account, keys, building facility badge.

5. Remote access

Suspend remote access capabilities, i.e.: smartphones, VPN accounts, tokens...

6. Seizure

Seize all the professional computing device of the suspected insider.

CONTAINMENT

Case 1: abnormal activity

If nothing malicious or fraudulent is confirmed yet, two investigations should start right now:

- forensics investigation on the computing devices of the suspected insider
- log investigation on different audit trails components

Use the IRM 02 or 03 depending on the operating system.

Case 2: malicious / fraudulent activity

If malicious or fraudulent behavior is already confirmed, think about file a complaint against the suspected insider.

In this case, do not take any further technical actions. Provide the legal team or law enforcement officer all requested evidence and be ready to assist on demand.

If collateral damages can result from the abuse, be sure to contain the incident impacts before making it public. Be sure to inform authorities if required.

Prepare a communication plan with the communication team (customers, partners …)

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

The remediation part is limited in case of an insider abuse. Following actions can be considered depending on the case:

- Take disciplinary action against the malicious employee (or terminate the contract) and remove all his/her credentials
- Review all programs or scripts made by the insider and remove all unnecessary codes
- Review administration tasks (IT Team)

Involve implicated providers and law enforcement services and regulators if required.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

If the incident has not yet been made public, make sure to notify all the impacted stakeholders (customers, concerned partners …) and required authorities. This communication must be made by top management in case of huge impacts.

Eventually warn your employees or local teams about the issue to raise awareness and harden security controls.

Roll back on the fraudulent operations committed by the insider.

For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRMXXX

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

An incident report should be written and made available to all applicable actors.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

Some improvement might be especially valuable considering insider abuse:

- Authorization process improvements
- Controls improvements in the organization
- Awareness on fraud and malicious activity