Preparation 1

Objective: Establish contacts, define procedures, gather information and get familiar with intrusion detection tools to save time during an attack.

Intrusion Detection Systems

- Ensure that the monitoring tools are up to date;

- Establish contacts with your network and security operation teams;

- Make sure that an alert notification process is defined and well-known from everyone.

Network

- Make sure that an inventory of the network access points is available and up-to-date;

- Make sure that network teams have up to date network maps and configurations;

- Look for potential unwanted network access points (xDSL, Wifi, Modem, …) regularly and close them;

- Ensure that traffic management tools and processes are operational.

Baseline traffic

- Identify the baseline traffic and flows;
- Identify the business-critical flows.

Identification 2

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Sources of detection:

- Notification by user/helpdesk;

- IDS alert;

- Detection by network staff;

- Complain from an external source.

Record suspect network activity

Network frames can be stored into a file and transmitted to your incident response team for further analysis.
Use network capture tools (tshark, windump, tcpdump…) to dump malicious traffic. Use a hub or port mirroring on an affected LAN to collect valuable data.
Network forensic requires skills and knowledge . Ask your incident response team for assistance or advices.

Analyze the attack

- Analyze alerts generated by your IDS;

- Review statistics and logs of network devices;

- Try to understand the goal of the malicious traffic and identify the infrastructure components affected by it;

- Identify the technical characteristics of the traffic:
    - Source IP address(es)
    - Ports used, TTL, Packet ID, …
    - Protocols used
    - Targeted machines/services
    - Exploit(s)
    - Remote accounts logged in

At the end of this step, the impacted machines and the modus operandi of the attack should have been identified. Ideally, the source of the attack should have been identified as well. This is where you should do your forensic investigations, if needed.

If a compromised computer has been identified, check IRM cheat sheets dedicated to intrusion.

Containment 3

Objective: Mitigate the attack effects on the neighbouring IT resources.

If the issue is considered as strategic (sensitive resources access), a specific crisis management cell should be activated.

Depending on the criticality of the impacted resources, the following steps can be performed and monitored:

- Disconnect the compromised area from the network.

- Isolate the source of the attack. Disconnect the affected computer(s) in order to perform further investigation.

- Find acceptable mitigation measures for the business-critical traffic in agreement with the business line managers.

- Terminate unwanted connections or processes on affected machines.

- Use firewall/IPS rules to block the attack.

- Use IDS rules to match with this malicious behaviour and inform technical staff on new events.

- Apply ad hoc actions in case of strategic issue:

    - Block exfiltration destination or remote location on Internet filters ;
    - Restrict strategic file servers to reject connections from the compromised computer;
    - Select what kind of files can be lost / stolen and restrict the access for confidential files;
    - Create fake documents with watermarking that could be use as a proof of theft;
    - Notify targeted business users about what must be done and what is forbidden;
    - Configure logging capabilities in verbose mode on targeted environment and store them in a remote secure server.

Remediation 4

Objective: Take actions to stop the malicious behaviour.

Block the source

■ Using analysis from previous steps identification and containment, find out all communication channels used by the attacker and block them on all your network boundaries.

■ If the source has been identified as an insider, take appropriate actions and involve your management and/or HR team and/or legal team.

■ If the source has been identified as an external offender, consider involving abuse teams and law enforcement services if required.

Technical remediation

■ Define a remediation process. If necessary, this process can be validated by another structure, like your incident response team for example.

■ Remediation steps from intrusion IRM can also be useful.

Test and enforce

■ Test the remediation process and make sure that it properly works without damaging any service.

■ Enforce the remediation process once tests have been approved by both IT and business.

Recovery 5

Objective: Restore the system to normal operations.

1. Ensure that the network traffic is back to normal
2. Re-allow the network traffic that was used as a propagation method by the attacker
3. Reconnect sub-areas together if necessary
4. Reconnect the area to your local network if necessary
5. Reconnect the area to the Internet if necessary

All of these steps shall be made in a step-by-step manner and with a technical monitoring.

Aftermath 6

Objective: Document the incident's details, retail collected data, and identify the improvements.
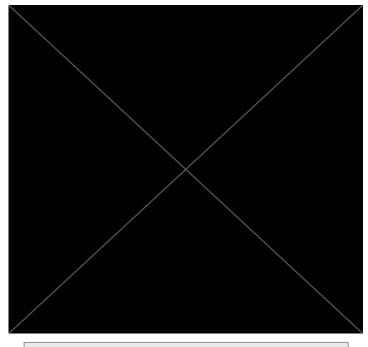
Report

A report should be written and made available to all of the actors.
The following themes should be described:
- Initial cause of the issue
- Actions and timelines
- What went right
- What went wrong
- Incident cost

Capitalize

Actions to improve the network intrusion management processes should be defined to capitalize on this experience.

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)

IRM can be shared with all SG staff.

Remember: If you face an incident, follow IRM, take notes and do not panic. Contact your CERT immediately if needed.

Incident handling steps

6 steps are defined to handle security Incidents

Preparation: get ready to handle the incident
Identification: detect the incident
Containment: limit the impact of the incident
Remediation: remove the threat
Recovery: recover to a normal stage
Aftermath: draw up and improve the process

IRM provides detailed information for each step.