IRM #0
GENERIC

Guidelines to handle a generic incidents
Version 1.0

INCIDENT DEFINITION

"Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein."
(NIST)

ABSTRACT

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

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

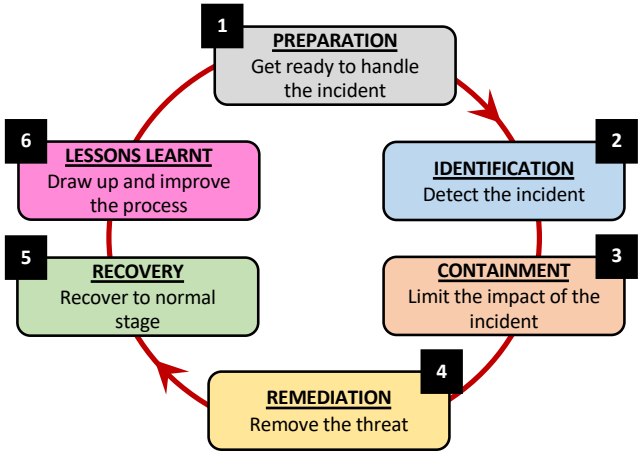
Remember: If you face an incident, follow these instructions, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

_____

_____

INCIDENT HANDLING CYCLE



1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

To prepare for most incidents you should consider the following actions:

- Document a list of key contacts both internally and externally. These are the people you will need assistance with technical, legal or approval questions.
- Ensure you have an accurate asset list/inventory with enough information about their location, purposes, status and owner
- Ensure all your key assets generate enough security logs (i.e.: at least 30 days but ideally 90+ days)
- Ensure you have access to those logs and that they are monitored
- Ensure your key assets are up to date
- Ensure your key assets are backed up
- Ensure the configuration of those key assets are documented, as you may have to reinstall everything from the ground up
- Although not a silver bullet, ensure most of your privilege accesses are protected with MFA
- Ensure your have a list of forensics / incident investigation toolset up to date and available, this should cover software and hardware equipment
- Conduct incident simulations regularly and review lessons learnt
- Subscribe to security mailing lists (vendors, opencve, SANS, etc) and keep a general awareness of the security scares/incidents happening in the world and they may affect you
- Identify 3rd party companies that may assist you if you do not have the resources in-house
- Document your incident response and handling procedures
- Communicate your incident response and handling procedure to the relevant staff
- Set up incident communication/contact mailing lists or chat group
- Raise basic incident response behaviour awareness among all your staff

2 IDENTIFICATION

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

Most incidents are detected through the following activities/medium:

- Unusual system or application behaviour
- Users access being blocked
- Users receiving unusual requests (phone or email)
- Email disappearing or not being responded too
- Security tools alerts
- Network suspicious activities: IDS, Firewalls, etc
- Host suspicious activities: local system logs
- Application suspicious activities: application logs

To identify a possible incident:

- Investigate the impacted asset for
    - Suspicious logged activities
    - Suspicious files
    - unusual processes
    - New registry key or configuration files
    - recent changes in config files
    - user browsing recent activities and download
- Conduct a security scan for known vulenrabilities and/or malware (Nessus, Nexpose, etc.)
- Update the relevant End Point protection software or A/V and run a full local scan. Consider using another 3rd party free software (i.e.: Emisoft, Sophos, etc) to do that offline, in case the local A/V has been compromised
- Threat intelligence source
- Security mailing list and Press alerts
- User reporting an issue
- SIEM/SOC alerts: a centralised and automatically aggregate and monitored security log system will help identify any potential attacks.
- An IDS will also greatly help you detect attacks and get automated alerts.
- "New" network and system behaviour analytics tools can also help identifying an issue.

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

Containing an incident will depend of its nature, the following actions are often used:

- Unplug the asset from the network
- Establish an incident communication group to coordinate your response. It can be as simple as an email thread or as advanced as a war room with side channel way of communication
- Design an incident coordinator who will manage the incident response
- Decide if you should switch off or not the impacted asset. Most of the time you should keep it running so you can analyse the issue further.
- Ensure you preserve evidence as much as possible as you investigate and contain the incident
- Save and extract your logs, now, before they get deleted and not just the logs of the impacted system but also all around it: email system, firewall, routers, AD logs, etc.
- Stop any suspicious activities (network, process, service, etc): Kill the process, block the email, black list the domain, etc
- Monitor your network and other systems to ensure they are not impacted, if they are you will need to further segregate them from the systems that are not impacted
- Change any passwords related to the impacted systems and user and enforce MFA
- Advise your management, IT staff and users of any potential future impact. You do not need to provide details, but you need to warn your users of any relevant suspicious emails, files, behaviour, etc. So they do not get impacted as well

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

- Conduct a more thorough investigation that you started in the previous steps
- Start by creating a "super time line": a timeline of event so you can gradually draw a clear picture of what is happening/happened
- Remove the suspicious program/services/process
- Review any persistent process or program
- Windows:
  - registry
  - startup files
  - services
- Unix
  - Services
  - Daemons/Agents
  - startup files in shell config
- Applications:
  - Configuration
  - users
  - rules
- Contact your security vendors for assistance
- Reach out to your security community and group for extra information on the incident
- Research relevant Indication of Compromise (IOC) to gain further knowledge of what needs to be done

5 RECOVERY

Objective: Restore the system to normal operations.

- Analyse the route cause of the incident and any potential backdoor
- Ensure the impacted system is fully cleaned from the attack – you may also have to inspect all your systems
- If this was a system compromise you may want to restore from a known safe backup or reinstall from the ground up if you have any suspicions of residual risk or if you haven't identified the root cause (but this may remove all evidences!)
- Ensure the system is fully patched and protected (F/W rules, AV, apps version, user access, rules, etc)
- If this was an application, review your application configuration, patch and access
- If this was because of a flawed process/awareness then review and communicate

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report

An incident report should be written and made available to all of the stakeholders.
The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve fraud detection and protection should be defined to capitalize on this experience.