Plan: security incident management

Author: Graciela Martínez
Edition: Communications Area
Department: Technology Area

November 2023

lacnic
www.lacnic.net

Purpose

The purpose of this document is to share a brief summary of the basic stages involved in defining a general plan for implementing security incident management in an organization. Having a defined plan helps effectively respond in case of a security incident.

Preparation Stage

- Establish the CSIRT
- Develop a security incident response plan: identify, advise, mitigate, and recover
- Establish a mechanism for reporting security incidents, both for the target community as well as for other interested parties
- Define incident taxonomy and their level of severity
- Define a procedure for triaging reports
- Define a communication plan for internal and external stakeholders; this plan should include authorized spokespersons and consider the image of the organization
- Train staff so they know how to identify potential threats and how to report security incidents
- Prepare an inventory of critical assets

Identification Stage

- Detect events and incidents: implement a monitoring system, centralize logs, implement intrusion detection systems

Containment and Eradication Stage

- Identify affected system(s) and take effective measures as soon as possible to prevent further damage
- Analyze whether legal notices are required
- Initiate the corresponding documentation, creating a timeline with the order of events
- Prepare communications, inform those who may be affected, and notify any other relevant parties
- Investigate the security incident to identify the causes that enabled the attack, assess the extent of the damages caused, examine the potential compromise of other systems, and analyze previously undetected potential vulnerabilities
- Eradicate the cause of the incident (e.g., remove malware, apply patches, change passwords, assess the effectiveness of event traceability, perform forensic analysis where and when appropriate, search for artifacts for further analysis, etc.)
- Document the reasons for the incident, the actions that were undertaken, and any facts that may be relevant to the proper understanding of the incident

Recovery Stage

- Restore affected systems as they are corrected
- Restore data from backups according to the organization's plan (if necessary)
- Implement new controls and measures identified during the investigation

Post-Incident Assessment Stage

- Review the documentation generated during the previous stages and add any information that might serve for future reference
- Document the lessons learned:
    - Incident management strengths and weaknesses
    - Assess whether it is necessary to prepare a training plan based on the characteristics of the incident that was analyzed
    - Assess whether it is necessary to update the management plan

Communication Plan

Having a well-defined and agreed-upon Communication Plan within the organization is very important. During the incident management process, appropriate communications must be issued according to this plan.

Broadly speaking, the following aspects should be considered:

- Communicate internally within the organization during all stages of the incident management process, considering the specific information requirements (need-to-know) of each role
- Communicate to external stakeholders as required by existing regulations and their specific information requirements (need-to-know)
- Establish a plan for managing press involvement if necessary
- If applicable:
    - Issue legal notices
    - Report to law enforcement agencies

- After concluding the security incident management process, prepare an executive report on the incident to be submitted to the organization's management and, if applicable, to its Board of Directors. This report is separate from any communications that may have occurred during the various stages of incident management.