Case 4: Incident Response
Group 5

Fatima Bayloun
Sandra Börjesson
Muhammad Arsalan Khan Mughal
Nibha Priyadarshini

29th April 2022

1. Incident Classification

Knowing that the incident concerns an authenticated account that "belongs to one of the employees at the financial department that has access to the records of all registered accounts", we can classify it as a ***level four-severe incident*** (very serious incident) according to the ISO/IEC 27035-2 classification. The financial department is a crucial business unit and the breached accounts or files contain personal data, and payment details (cards, accounts, etc..). This could result in financial loss & loss of personal data. However; it is not clear whether the authorized user is the employee himself (insider) or an attacker who managed to gain access to the employee's laptop.

2. Incident Management Process

In accordance with the incident management process presented in NIST SP800-61, the following illustration shows the 4 phases that will be followed in this case.

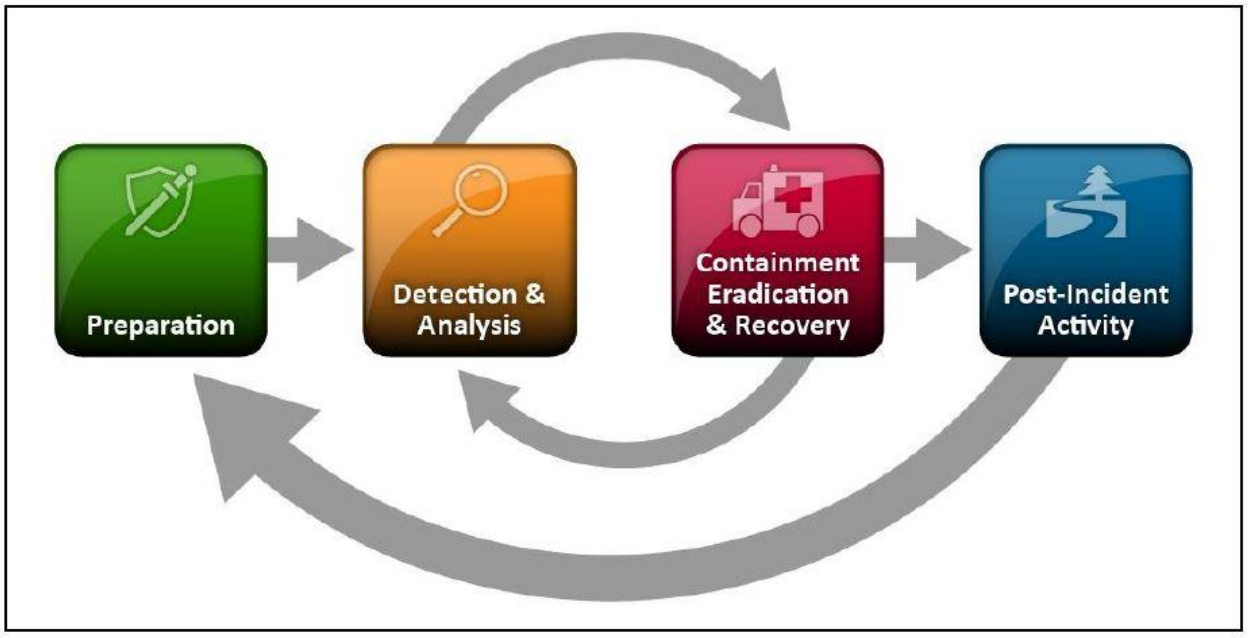

Figure 3-1. Incident Response Life Cycle

Phase 1. Preparation

- Preparation to handle incidents

The first phase is focusing on preparation, which is ensuring that the components in the company are secured enough and that the company has a plan on how to continue if an incident happens.

<u>Communication and facilities</u>

The company should include these parts to ensure sufficient protection of their facilities and communications;

- Contact information where they can identify all employees in their company. The contact information should be continuously updated and be stored safely inside the company.
- It can be seen in the company that they have an incident response team, and that their information is being logged, however, they need to ensure that the response reporting exists for all users to report incidents instantly and anonymously.
- Encryption software should be used for communications among internal and external parties. Their internal guest network is being encrypted with the use of WPA2 enterprise, which is a secured option and uses AES. It should be configurated correctly to ensure that their information on the internet is being secured enough.

Hardware and software

The company should include these parts to ensure sufficient protection of the hardware/software.

- Forensic workstations or backup devices. The company does have a backup for primary data, and backup power supplies. However, they have not mentioned having a forensic workstation.
- Laptops for analyzing data. They have an incident response team, which is good.
- They should have the policy to ensure that chain of custody is being documented correctly.

Resources

The company should include these parts to ensure sufficient protection of their resources

- Port list, where the company should have documented commonly used ports and trojan horse ports
- Documentation for the company's protocols, intrusion detection, and antivirus products.
- Cryptographic hashes should be existing for critical files.

Mitigation Software

The company should include these parts to ensure sufficient protection for their mitigation software.

- Access to images of the installation, to use for restoration and recovery. This is not mentioned in the information provided by the company.

- Preventing incidents -

The protection of the organization is essential. Here we will mention the main practices to ensure security for their assets such as networks, systems, and applications.

Risk assessment - A risk assessment should be done and should be documented in the company. It should be continuously updated and analyzed. After an incident occurred, their risk assessment should be overviewed. For example, this incident regarding high

usage of CPU power on the backend servers should be documented and should be updated with the risk assessment.

Host security, -granting users privilege, standard configuration, and keeping the users patched. This has been mentioned by the company, where they have access controls to their internal network.

Network security, - The network should be configurated in the company. They use VPN and they log the network. They should use firewalls, routers, and switches.

Malware prevention - They have anti-malware software on each of the employees.

User awareness and training - They have an IT department that should be aware of the technical security. However, they should have the training for all employees and it should be done continuously.

Phase 2. Detection & Analysis

- Attack vectors
  Gathering information to identify the possible attack methods used in this incident: removable media, attrition (brute force attack), Web (stealing credentials:cross-site scripting attack), email (malicious attachment), Impersonation, Improper usage (being an insider violation), and loss/theft of equipment.
  > These all are possible attack vectors that should be taken into consideration during the analysis.
- Signs of the incident
  1. Unusual-High CPU power usage at a database backend server
  2. System access & file transfer outside working hours
- Sources of Precursors and Indicators
  1. People: System Administrators + Network administrator+ anyone from IRT (Incident response team)
  2. Automated alerts: Network-based and host-based IDPSs and system log analyzer
- Incident Analysis
  Scope: File transfer: multiple instances of /bin/scp - a file transfer program (Same to Unix command cp which uses SSH to transfer Files
  Who : Employee in the financial department
  How: Impersonation or improper usage
  When: At 03.41 hours (local time)
  Where: Database backend servers reside on a Solaris machine

These details can lead us to identify a clear high-risk incident, with a clear scope: unusual usage (CPU & file transfer) and unusual time. A more technical analysis shall be done to further correlate the available data, packet sniffers can also be used to collect additional information.

- Incident Documentation
  From the time of detection, the team will immediately start recording and documenting all the facts (e.g. logbook)
- Incident prioritization
  According to (NIST SP800-61): “Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process.”
  As the organization can get many incident alerts each day, it is important to prioritize the incidents according to clear factors:
    - Functional impact
    - Information impact
    - Recoverability from the incident

> if we follow these factors to prioritize the identified incident: we can set a “ high” priority for the 3 above mentioned factors.

- Incident notification
  Appropriate individuals(main stakeholders) are to be notified immediately about the incident. (Appropriate individuals are usually stated in the organization’s incident handling policy/strategy). E.g. CIO, Head of security, head of IT.

Phase 3. Containment Eradication & Recovery

- Legitimate business loss and high damage to reputation are expected. Since the laptop from which data theft is happening has access to all the user accounts.
- Tailored remediation strategy and procedures to stop incident from overwhelming resources or increasing the damage
- Decision making required:
    - Shut down a system
    - Disconnect the system from a network
    - Disable certain functions (file transfer)
    - Decrease the access rights of the user id of the employee which has access to the user accounts to decrease the consequences
    - Encrypt the files which are going out of the employee mail id or employee system
- Criteria for deciding on appropriate strategy:
    - Potential damage to and theft of resources
    - Need for evidence preparation
    - Service availability (Network connectivity, services provided to external parties)
    - Time and resources needed to implement the resources
    - Effectiveness of strategy
    - Duration of solution (Temporary workaround, emergency workaround, permanent solution)
- Gather more information/evidence and handling
    - Take an image of the laptop of the employee from where data theft is happening. The assumption is there is a way to take the image of the system online without employees being informed
    - Take the list of files that are being transferred

    - Identify the list of user accounts impacted by this file transfer
    - Capture information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
    - Maintain chain of custody of the evidence gathered
        - Name, title, and phone number of each individual who collected or handled the evidence during the investigation
        - Date and time
        - Locations where evidence was stored
- Identifying the attacking hosts
    - Focus is more on minimizing the business impact
    - Check the email id to which files are being transferred or note the location where the files are uploaded somewhere online.
- Eradication and recovery
    - Disable laptop, user account, email id
    - Eliminate the components of incidents
    - Restoring the system from a clean backup

Phase 4. Post Incident Activity

The organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents. Trust is lowered after the incident.

> Lessons Learned meeting is one way to discuss what happened (among the IRT) , aiming to learn and improve and use the collected data to prepare for future similar incidents.
The result of this meeting shall be a documented closure of the case/incident as well.

---

3. References

ISO/IEC 27035-1 (Principles of incident management)
ISO/IEC 27035-2 (Guidelines to plan and prepare for incident response)
Incident Handling Guide SP800-61