Case 4 - Incident Response Group 1

Carl Sundelin
Karin Säberg
Hamid Farajisarkati

How would you classify the incident?
Deliberate
Incident Class: Intrusion
Incident Type: Privileged account compromise
“This can have been caused remotely by a known or new vulnerability, but also by unauthorised local access.” according to eCSIRT.net security incidents taxonomy.

How would you assess and resolve the incident? Describe the steps (in accordance with the incident management process presented in the lecture) and actions taken.

Incident management process

Plan and Prepare

- Plans that were in place from before the incident should be followed. They should confirm that the proper personnel is dealing with the issues that are taking place and that they are resolved quickly

Detect and analyse

- Determine whether there is only one account that has been compromised or if many are already. Is it an authorised user doing it or has their account been compromised?
  - Has the same account been used to do other suspicious activities in the past?
- Gather the logs(audit logs) from the relevant servers, especially the Windows Servers handling user profiles and authentication of staff computers
  - Collect the employee laptop that was used during the incident as soon as possible
  - Collect network logs
  - Collect logs from the Solaris machines
- The incident impact is analysed
  - The scope is considered limited as it appears to be contained to one user copying files
  - The business impact is considered severe as customers are likely to consider this a breach of privacy and be worried about what information has leaked. This could give the company a bad reputation and lose customers. Additional fines may be levied against the company for breach of personal information legislation (GDPR)

- Check the collected data and determine if an account was compromised. If it was, check other accounts for similar attacks that may have been missed, to ensure that there is only one account that is compromised
- Collect all the information about the incident into one incident report

Containment, Eradication and Recovery

- Containment
  - Short-term containment - isolate the problem to not affect unaffected systems
    - Disable and/or remove all permissions authorised to the account causing the incident
    - Make sure that the games that are being run on the VMs are not affected by the increased CPU power usage causing problems for customers
  - System-backup - make sure it isn't infected with the same issues/backdoor/vulnerability
    - Create forensic copies
    - Compare the file systems from after the transfer of data to a back-up copy that was taken before the incident to ensure nothing has changed
    - As the incident was started by an authorised account restrict access to the backend servers during the investigation, in case other accounts are affected
  - Long-term containment
    - Take offline → eradication
      - Move unaffected systems from the affected server to another so that the targeted server can be taken offline to eradicate the issue

- Eradication
  - Remove the incident account or otherwise ensure it is once again secure
  - Ensure that if a weakness on the user laptop was utilised all company computers with the same weakness is patched and hardened
  - Find the weak spot in the defences by understanding how the attack took place
  - Ensure all the malware/artefacts that are left behind are removed from the newly hardened system

- Recovery
  - Ensure that the copied files have not been manipulated in any way by comparing them to the ones from the latest backup/logs relating to the different accounts
  - Proposed countermeasures to ensure it won't happen again
    - Limit copy access to a few accounts, or have a second person approve the copy request
    - Limit access to need-to-know
    - Limit access to read-only when access is needed but write access unnecessary

Closure

- Making sure that the incident is taken care of and that the operations are back to normal again
- Evaluate if the system is secure
- Has the incident been handled?
    - If no - start from the detection and analyse step and go through each part again
    - If yes - finalise the report and prepare for the post-incident meeting and follow-up

Identify and propose post-incident actions.

Re-assess the existing plans and procedures to encompass the new attacks and look for other similar attacks that can take place in the network

Lesson learnt and post-incident meeting

- Review the incident response process
    - Evaluate the incident response process
    - What about the process can be improved?
- Discuss Business Continuity Plan, IT Service Continuity Plan, and Business Impact Analysis

Business Continuity Plan

- Re-assess the organisational threats and risks of them occurring
- Education requirements of personnel to identify and stop similar attacks in the future
    - If it was the laptop user's who fell victim to social engineering or similar: ensure more and better information security training of employees

Communications & Media plan

- Follow laws regarding personal information leaks if any have taken place (e.g. GDPR)
- Follow company policies regarding contact point, bulletins for emergencies, protective actions, public advice and actions guidelines, frequency of communication

IT Service Continuity Plan

- Further system hardening
- If a vulnerability or weakness was used to gain access to the user account: why were the computers not up to date or otherwise hardened?
- Can the system be reimaged, and hardened with patches to prevent similar attacks?

Business Impact analysis

- Determine what systems were impacted by these attacks, and how critical they are to the business
- Determine the resources needed to recover from the incident

Preventative Controls and Contingency Strategies

- Review the existing documents covering the controls and strategies
    - Check backups are not infected and implement similar patches to these systems
    - Replace equipment that may have made it easier to compromise the system/network
    - Make changes to the contingency plan depending on the trustworthiness of the employee whose account caused the incident
    - Set limits for users with access to critical data
        - Access time limit (Work hours)
        - Resource usage limit (one member from the operational and security IT departments need to approve of commands and large operations on the servers)