Preparation: Incident Response Plan

Having an incident response plan (IRP) can make all the difference when responding to a security incident. Having a well documented plan for IT and security staff can ensure that the response process is clear and defined, preventing confusion which costs the organization valuable time. Incident response plans need to be constantly updated and training should be maintained constantly to ensure all employees that could be involved with incident response are capable of performing their duties.

IRPs are typically split into the following six sections:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

You can view some sample incident response plans at these links:

- Carnegie Mellon University—including definitions, roles and responsibilities, methodology, incident response phases, guidelines for insider threats and interaction with law enforcement, and documentation.
- Wright State University—including scope, response steps, usage of security tools, and an intrusion checklist.

PREPARATION

This is arguably the most important stage, and requires the most attention, not just when writing the plan but also ensuring that team members are continually trained on their responsibilities. We can split this section into three main phases:

- Developing response plans for different incident types and running simulated scenarios to evaluate how the incident response team responds, training them for the real thing.
- Ensure that all resources needed by the incident response team are approved and ready to use, such as: laptops, notebooks, software tools, forensic equipment, training, and the ability to abandon normal responsibilities when an incident occurs.
- Continually train and evaluate the performance of incident response team members to ensure they are capable of completing their duties defined in the response plans. For security analysts this could be analyzing and collecting information about the incident, for forensic analysts it could be the acquisition and preservation of digital evidence, and for employees from PR/communications departments, this could be drafting notifications to the press or affected stakeholders.

IDENTIFICATION

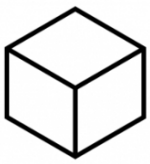
This section focuses on the ability to identify and analyze an incident. It will provide guidance on how to report an incident, and what information needs to be gathered and included such as:

- When did the incident occur?
- Who discovered it? (Whether this is a member of the security team or another employee that reported unusual activity)
- How did they discover it?
- What systems or business units have been affected?
- Does it affect the organization's ability to operate?
- What is the scope of the incident? (How many systems are affected, what was the initial point of entry, what damage has been caused?)

Once an incident has been discovered, organizations may choose to assign two values to help with prioritization, especially if multiple incidents occur simultaneously:

- **Criticality level:** How fast does the response need to be?
- **Impact level:** How long will the incident impact business operations?

CONTAINMENT



It's crucial to contain an incident so that it can't spread and affect more systems causing additional damage and disruption. This section of the IRP should outline what actions should be taken to contain the incident by taking actions such as: disconnecting compromised devices from the internet preventing remote access or powering off systems.

This stage is extremely important, as this is when digital evidence will be collected and preserved for later analysis, so containment measures need to be carefully considered, as powering off a system would result in losing crucial evidence that could be in volatile areas such as memory. Careful guidelines and procedures should be documented to allow for straightforward evidence acquisition and containment measures, both short-term and long-term.

Backups should be kept so that affected systems can be taken down and the backups can be used in their place, allowing normal business operations to continue.

ERADICATION

Now that the incident is unable to spread to additional systems, analysis activities can be performed to work out exactly what happened. The MITRE ATT&CK framework can be used to work backward and potentially identify previous steps of the attack. The analysis will be conducted using methods such as looking at packet captures, reviewing logs from a SIEM, and working until the root cause has been identified. Guidelines should be provided to state how the analysis should be conducted, and appropriate resources should be provided such as software tools.

Once found, it's time to start removing malicious artifacts such as the presence of malware, any changes to systems and settings made by malicious actors, and ensuring that any methods to retain persistence are removed so actors are not able to get back into systems.

At this point defensive measures should be taken to ensure that this type of incident can't happen again by hardening systems, applying patches, and empowering automated defenses such as NIPS and HIPS using indicators of compromise gathered throughout the investigation. By creating run-books for different incidents, incident responders can quickly evaluate the suggested measures and implement them quickly to prevent additional incidents occurring.

RECOVERY

This stage is all about returning business operations to normal by moving affected systems back to production environments now that they have been cleaned and hardened. Guidelines should be provided for ensuring systems are no longer infected, and how to properly return them back to business operations. An example of this could be a website that has been compromised via web shells, giving attackers access to the server itself. In this case, a backup server could be used to host the main site temporarily. Once the infected server has been cleaned and all malicious presence removed, the site can be hosted on the primary server again.

LESSONS LEARNED

Once the investigation and response are complete, a meeting should be held that includes any stakeholders involved in the incident. The focus of this meeting should be to recap exactly what happened, specifically what went well, and how could the response have been improved. Lessons learned from both simulated and real events will help strengthen systems against any future attacks. The strengths and weaknesses of the response should be discussed and used to drive change, such as rewriting documentation including policies and procedures, or securing more budget if needed for additional tools or personnel.

CONCLUSION

Going through an incident can be tough, but learning from mistakes and gaps in security can enable the security team to improve defenses and raise the security posture of the organization. An effective incident response plan needs to constantly be updated to remain valid and useful resource. Training also needs to be completed routinely so incident response team members remain effective and ready to get to work. Tabletop exercises and simulated attacks can be a great tool for maintaining a high level of readiness, involving all appropriate stakeholders.

Previous Topic
Mark Complete
Next Topic
Back to Lesson