Elizabeth Martinez

Sriven Srilaksmi

Asim Chaudhary

In class Exercise 5

Evaluating the NIST Incident Response Life Cycle:

Analyze the stages of the NIST Incident Response Life Cycle: preparation, detection, containment, eradication, recovery, and post-incident activity.

Ans- 1. Preparation- The business identifies and develops an incident management plan, which is able to identify an incident within the organization's environment. This includes preparation by identifying the different malware attacks and what would be the impact on systems and to make sure an organization has tools for incident response and security controls to prevent an incident from occurring.

2. Detection and Analysis - gathering data and analyze it to see if there is any clue to trace the origin of an attack. During this stage, the analysts identify the nature of the attack, its consequences on the systems, and the possible impact on the business.

3. Containment- In this step all possible methods are used in order to prevent malware or viruses from spreading.

4.Eradication- After containing the security issue at hand, the next step is to eradicate the malicious code or software from the environment. This could be through utilizing antivirus tools or other forms of manual removal. It will also involve making sure that all your security software is current to help prevent a future occurrence.

5.Recovery: This would involve restoring all systems to their pre-incident state after the malware has been removed, including restoring data from backups, reconstructing infected systems, and re-enabling disabled accounts.

The final phase of the incident response life cycle is to perform a postmortem of the entire incident . This helps the organization understand how the incident took place and what it can do to prevent such incidents from happening in the future. The lessons learned during this phase can improve the organization’s incident security protocols and make its security strategy more robust and effective.

Reference-
https://www.eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/

Which stage do you believe is the most impactful for minimizing damage during an incident, and why? Use a real-world example, if available, or create a hypothetical scenario where focusing on this stage would significantly enhance incident management.

Ans- Containment is the most impactful for minimizing damage during an incident. It stops the attack from spreading and escalating further, immediately putting organizations in control before an attacker can create irreparable damage. Containment involves the isolation of compromised systems, access restriction, and temporary fixes that may stop an attack from further escalating while full recovery commences.

Real world scenario- Wannacry ransomware spread rapidly across unpatched systems. It exploited the EternalBlue vulnerability in the SMB port which Windows uses for file and printer sharing over a network. The best security strategy against ransomware is a mix of prevention, detection, and recovery capabilities. The spread of the ransomware could have significantly been reduced if the organizations had isolated the infected devices and restricted network access once they identified the behavior of the malware. In other terms, network segmentation limits lateral movement, ensuring an attack is confined to initial systems rather than paralyzing whole networks.

https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

https://www.cyberark.com/resources/blog/wannacry-deconstructed-five-ways-to-mitigate-ransomware-risks

Distinguishing Incident Response and Disaster Recovery

-Research the distinctions between Incident Response and Disaster Recovery plans, exploring why it's essential to have both.

An incident response plan is a plan created in order to prepare for a cybersecurity plan. This plan includes identification of threats that are most likely to occur and how one can prevent them from occurring or how to respond if that attack were to happen on that system. An incident response plan is important to have because in the event of an attack it is always best to act fast and quick. This incident plan will be the outline on the steps needed to take to stop the attack as well as insure you are able to plan ahead and make sure you have the correct resources to resolve the issue

A disaster recovery plan is the plan that is put in place to have preparation for faster recovery after a cybersecurity attack has occurred. A disaster recovery plan is important to have because it prepares a business or user on how they will recover information in the event it is lost during the attack. It also prepares a business or user on how they should continue to run their operations until they have fully recovered.

https://www.loginradius.com/blog/identity/difference-between-incident-response-disaster-recovery/

-If specific examples aren't accessible, describe a hypothetical scenario where each plan is implemented to address a cyber incident or natural disaster. Highlight the unique roles each plan plays in ensuring organizational continuity and resilience.

A scenario where an incident response or disaster recovery plan is implemented to address a natural disaster would be if there was a strong earthquake.

In an incident response plan the first step of the plan could be to ensure the safety of its employees which can be done by using safety protocols that were made sure they were up to date when the incident response plan was written. The next step could be to check the condition of the building. This can include by using an incident response team that was stated in the incident plan. This team could check not only the building's structure but also to see if there are any hazards or IT equipment that need replacement. The incident response plan should have prepared the company by making sure they have the resources to take actions fast and smoothly.

In a disaster recovery plan the disaster recovery plan should include how the company would restore its data and what group of people would be responsible for that in the event of an earthquake. This disaster recovery plan should also have scenarios on what to do in case there is a really bad disaster. This can include being set up to be able to have its employees work remotely so that the company can continue to run and their employees can continue to work on tasks that are essential to keep the business running.

Business Impact Analysis - (BIA)

Business Impact analysis is the first step of the Contingency planning processes and serves as an investigation and assessment of various adverse events can have on the organization.

BIA begins when risk management fails, and an attack has been successful. It then analyzes what kind of impact the threats had on the business. The BIA begins with the prioritized list of threats and vulnerabilities identified in the risk management process.

According to the NIST SP 800-34, the BIA is conducted in three stages.

1. Determine business/mission processes and recovery criticality.
2. Identity resource requirements
3. Identify recovery priorities for system resources.

For the first stage of BIA, we need to find which processes are critically important for business operations. We can use weighted tables for this analysis. After an organization considers recovery criticality, they must determine how much time it will take to recover resources. We can use metrics like RPO (Last backup point where data is usable) and RTO (How long it will take to recover). Once the processes that are affected are identified, we determine what resources each process requires to return to normal functioning. The last stage of BIA is prioritizing what needs to be recovered first, even within the most critical processes.

BIA is essential in contingency planning as it helps organizations allocate resources effectively, ensuring that **the most critical functions are restored first**. By understanding the potential impact of disruptions, organizations can mitigate financial and operational losses, safeguard customer trust, and maintain regulatory compliance.

Imagine a healthcare provider facing a ransomware attack. Through its BIA, it has identified health records are critical. With established RTOs and RPOs, IT teams focus on restoring health records. The BIA reduces recovery time, helping prevent adverse effects on patient care and ensuring compliance with healthcare regulations.

Reference : Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, 7th Edition.