INTERN CAREER

"WE SPEAK DATA"

CYBERSECURITY REPORT

TASK 2: INCIDENT RESPONSE

ZANELE NDLOVU

INTRODUCTION

The following report will use the business example we used in task 1 and it will provide an in-depth cybersecurity risk response for a fictional small business, called Easy Solutions Corporation (Rahmonbek, 2024). Easy Solutions Corporation, a small business specializing in software development, has been attacked by Attacker Group ABC. The group has initiated a phishing campaign aiming to contaminate the company's network with ransomware. That phishing email contains an apparent legitimate attachment that, when it is opened, automatically installs malware designed to encrypt confidential business data and demand a ransom for decryption.

The email is basically seen as a typical routine email from their trusted vendor, it is attached with the company's logo and a professional tone.

OBJECTIVE

The main objective of this task simulation is to examine the company's incident response plan and upgrade its ability to operate cybersecurity incidents. This includes detecting, containing, and mitigating a simulated ransomware attack that was launched by the ABC company.

SCOPE

The scope of this scenario will involve a handful of departments; it will involve HR, IT. It will also aim to cover technical and non- technical stuff.

INCIDENT DETECTION

Assigning interns roles within the incident response team.

We have an IT manager, IT intern and HR. They ensure that incidents are thoroughly responded to in an efficient way. The tasks have been assigned to in this specific way.

Duty assignment:

Themba, the IT manager, is the incident coordinator: Themba is in charge of overseeing the incident response. He makes sure that everyone is aware of their responsibilities and collaborates effectively to solve the problem.

Emily, the IT security intern, is the threat analyst. Emily delves into the analysis of the phishing email and its attachment. She determines the type of malware at play and the extent of the infestation.

Mike, the IT support intern: Mike intervenes on behalf of the impacted staff members. To prevent the infection from spreading further, he isolates any compromised PCs.

HR Intern Sarah, Communications Specialist: - Sarah is tasked with informing all staff members to the phishing attack. She also gives them advice on what to do in the event that they receive suspicious emails.

Initiate the Incident Response Plan:

- Themba activates the incident response plan, ensuring all team members follow their defined roles and responsibilities.

Contain and Mitigate the Incident:

• Emily looks into the malware to learn about its behavior and spread.

Mike separates the compromised devices to stop the infection from spreading.

• Sarah keeps in touch with every employee, cautioning them not to open any more suspicious emails or attachments.

• Using backups, the team collaborates to neutralize and lessen the threat and retrieve encrypted data.

Forensic Analysis

Understand the Root Cause:

- Emily will perform forensic analysis on the affected systems, examining the phishing email and malicious attachment.
- She identifies the malware's origin, its entry point into the network, and its mechanisms of action.

By identifying and addressing the fundamental causes of this phishing attack, the team can develop measures to avoid the incident from happening again. This does not only save time and resources for the company but also improves overall safety and performance in future.

Gather Evidence:

- Collect logs from email servers, endpoints, and network devices.
- Document the malware's behavior and the response steps taken.

Post-Incident Assessment

Review Effectiveness:

- The team reviews the incident response plan's effectiveness, evaluating how well the incident was managed.
- Analyze the time taken to detect, contain, and mitigate the attack.

Identify Areas for Improvement:

- Discuss lessons learned from the simulation.
- Identify any gaps in the incident response process and make recommendations for changes
- Update the incident response plan based on the findings to better prepare for future incidents.

Incidents can disrupt operations and cause delays. By addressing the fundamental problem, you may avoid these disruptions while also increasing efficiency and production.

By following this structured approach, Easy Solutions Corporation can enhance its preparedness for real-world cybersecurity threats, ensuring a robust defense against potential attacks from groups like ABC.

The journey doesn't end with mitigating a single incident. For Easy Solutions Corporation, each simulation is a step towards building a resilient cybersecurity posture. By continuously refining their response plans, conducting regular training sessions, and staying abreast of emerging threats, they transform vulnerabilities into strengths, ensuring they remain a step ahead of adversaries like Attacker Group ABC.

Conclusion: Embracing the Unseen Battles

In the ever-evolving digital landscape, the battle against cyber threats is ongoing. For Easy Solutions Corporation, the key to survival and success lies in vigilance, preparedness, and a proactive approach to cybersecurity. This guide not only highlights the importance of a structured response but also underscores the need for continuous improvement. By staying prepared, they can face the unseen battles head-on, protecting their digital assets and ensuring business continuity.

Understanding the Attack: An incident report details the malware attack, including its origin, method of infiltration, and the amount of damage caused. This information assists cybersecurity teams in understanding the attack vector and the strategies used by attackers.

Root Cause Analysis: By conducting a thorough investigation and recording the occurrence in a report, cybersecurity professionals can determine the source of the malware infestation. Understanding how the malware got into the system allows firms to resolve underlying vulnerabilities.

Mitigation and Recovery: Incident reports detail the methods taken to contain the malware attack and restore affected systems and data. This information is crucial for quickly restoring regular operations while reducing the impact on business continuity.

Legal and regulatory compliance: Many industries have laws or regulations requiring firms to report cybersecurity issues, such as malware attacks. An incident report provides as proof of compliance with these criteria and demonstrates due diligence in securing sensitive information. Improving Incident Response: By analyzing incident reports, companies can analyze the effectiveness of their incident response systems and find areas for improvement. Learning from previous occurrences allows cybersecurity teams to improve their response techniques and better prepare for future assaults.

Communication and Transparency: Incident reports facilitate communication among various stakeholders, including internal teams, senior management, customers, and regulatory bodies. Transparent reporting builds confidence and responsibility while demonstrating the organization's commitment to cybersecurity.

In summary, writing an incident report after a malware attack is critical for analyzing the attack, detecting vulnerabilities, limiting the effect, adhering to legal obligations, strengthening incident response skills, and maintaining transparency and confidence among stakeholders.