BUSINESS RESILIENCE AND INCIDENT MANAGEMENT

CHIJIOKE FRANKLIN EMEJURU

Project Overview: Improving Cybersecurity and Response Plans

This project focuses on improving the cybersecurity and incident response plan for Company A, a medium-sized financial service provider. The company is currently reviewing its plan to ensure it aligns with best practices, specifically the NIST SP 800-61 Rev. 2 framework. The current plan is outdated, lacking advanced tools for threat detection and a structured recovery process.

We analyse a real-world cyber incident (Mailchimp's 2022 breach) to understand how the company responded and suggest improvements for Company A. These improvements include better preparation for attacks, real-time threat detection, and standardised recovery procedures.

The project also discusses the role of different teams in protecting the company: Red teams (attackers who identify vulnerabilities), Blue teams (defenders who protect systems), and Purple teams (a mix of both). We recommend integrating these teams to create a stronger, more effective incident response plan.

1.0 INTRODUCTION

In a time of (volatility, uncertainty, complexity, and ambiguity), businesses must constantly adapt to a wide range of crises that could disrupt their operations and reputation. The ability of a business to withstand adversity and quickly bounce back from calamities is critical to its strategic success. People who don't understand the current organizational continuity models and don't prepare their firm effectively for VUCA risks might not make it through. When you say a business is resilient that means the organization has foresight to recognize potential risks with on-going size-up of the operating environment to prevent unwanted disruptions or crises from emerging. In the event of a malicious attack the ability to detect, respond and recover from the after effects in a timely fashion. There are frameworks in place to handle such scenarios such as the Incident Management Body of Knowledge (IMBOK). This helps to achieve business resilience. The NIST framework highlights a risk based approach towards cyber security which helps organizations in achieving resilience.

2.0 ORGANIZATIONS INCIDENT RESPONSE PLAN

2.1 Overview of the Company A Organization

Company A is a medium-sized financial service provider company which provides loan services and internet banking services. The organization's current Incident Response (IR) plan is being reviewed to determine whether it complies with the widely used incident response framework, NIST SP 800-61 Rev. 2.

2.2 Evaluation of Company A

The assessment focuses on the alignment of the organization's IR plan with NIST's four key phases which are Preparation, Detection and Analysis, Containment, Eradication and Recovery,

and Post-Incident Activities**.**

Preparation

Although the organization has a basic incident response policy that specifies who to call in the event of an attack, the policy is out of date and lacks specific procedures. Advanced threat detection technologies are absent, despite the presence of firewalls, antivirus software, and endpoint security solutions. NIST emphasizes thorough preparation.

Improvements to be made

-Regular training security awareness should be conducted

Detection and analysis

Basic monitoring tools were used for network activities and there is no real-time Security Information and Event Management (SIEM) system. Incidents are detected based on customer complaints or external alerts.

NIST recommends real time monitoring and automated detection equipment.

Recommended improvements

-Integration of automated threat intelligence systems

Containment, Eradication and Recovery

The organization follows ad-hoc containment practices, which vary depending on the incident occurring. Efforts to recover are lengthy because there is no standardized process for restoring systems. NIST recommends a standardized method of recovery and a well documented containment strategy.

Recommendations

-Development of incident playbook for incident response processes

Post- incident activity

Here Post-incident feedbacks are conducted informally, without structured documentation or feedback loops. information obtained is rarely integrated into future security measures, which limits the organization's ability to improve its IR capabilities.NIST emphasizes on the importance of post- incident activities, this helps in breaching gaps and in the improvement of response strategies (Sun *et al.*, 2023).

Recommended improvements

-Integration of feedback into security policies and practices

3.0 ORGANIZATIONS RESPONSE TO CYBER INCIDENT IN TERMS OF IR LIFECYCLE

Examining the cyber incident involving Mailchimp which occurred in the month of April 2022. This incident disrupted the flow of the organization's operations. Lots of personal information was breached and this was done with the use of social engineering (Ahmad *et al.*, 2021).

3.1 Mailchimp's incident overview

In April 2022, Mailchimp's security team identified unauthorized access on one of the tools used by Mailchimp's customer-facing teams for customer support and account administration. The attack was done with social engineering on one of Mailchimp's employees which gave them access to Mailchimp's accounts.

3.1.1 Mailchimp's response to the incident

Due to the attack Mailchimp took necessary measures to prevent future incidents. Which included the suspension of affected accounts within 24 hours of delivery and notified the affected users accounts.

3.1.1.1 Recommended improvements relating to Mailchimp's cyber attack using IR lifecycle

Preparation

This phase helps in detecting an incident in the organization’s environment. This step involves the identification of malware attacks and determining the impacts on the organization's systems .

Detection and Analysis

An incident response analysis is responsible for collecting and analyzing data to find clues to help identify the source of attack (Sun *et al.*, 2023b). Analysts utilize tools and indicators of compromise (IOC) that help track attacked systems (Capuano *et al.*, 2022).

Containment, Eradication and Recovery

Containment: This step is used to prevent the spread of malware or viruses.

Eradication: After containing the security issue, The malicious software needs to be eradicated with the use of antivirus or removal techniques.

Recovery: After elimination of the malware all systems will be restored.

Post-incident activity

This is the final phase of the incident life cycle. This helps the organization understand how the incident took place and what it can do to prevent such incidents from happening in the future.

3.2 Recommended improvements

-Development of a Clear Containment Strategy

-Establishment of a Continuous Improvement Process

4.0 STRENGTH AND WEAKNESSES OF INCIDENT APPROACH

4.1 STRENGTHS DISPLAYED BY THE ORGANIZATION

-Initial response effort by the organization

-Willingness to improve IR efficiency

4.1.1 WEAKNESSES

-Lack of dedicated IR response team

-Lack of security awareness training

The ransomware attack's success could be a sign of inadequate staff awareness and training (Liu *et al.*, 2024). Employees are more vulnerable to phishing attempts if they are not given enough training on how to spot phishing emails and other possible dangers. This reveals a lack of preventative procedures (Mazhar *et al.*, 2023).

4.2 STEPS TAKEN TO ENHANCE INCIDENT RESPONSES

Planning and preparation

Policies should be created and updated, Communication lines should be formalized and an Incident response (IR) team should be established

Detection and analysis

Use of monitoring systems, reviewing of logs and identification of attack indicators. Verification of security events should be done

Containment, Eradication and Recovery

Formalized prices for each attack should be done, threats should be contained and eradicated with the use of logical and physical means. Recovery this entails bringing all systems back to normal operational status.

Post-incident activity

The root cause of the incident should be improved, controls and security protocols should be updated. Feedback should be worked on to avoid future threats .

4.2.1 ROLES OF THE RED TEAMING AND BLUE TEAMING TRAINING

Red team (Offensive Security)

A red team approaches cybersecurity offensively. They comprise of individuals authorized to simulate an adversary's attack

Key roles of a red teamer

-Carrying out penetration tests.

-Managing phishing and social engineering.

Blue team (Defensive Security)

A blue team performs defensive cybersecurity tasks which include placing and configuring firewalls, implementing patching programs, enforcing strong authentication and ensuring physical security measures are in place.

Key roles of a blue teamer

-Monitoring the logs of all endpoints and services.

-Responding to security incidents in case of an attack

5.0 ORGANIZATIONS INCIDENT RESPONSE PLAN BASED ON THE BLUE TEAM OPERATIONS

After the post-incident review of the phishing based ransomware attack it was important to assess the effectiveness of the blue team's activity during the containment and recovery phases.

Containment phase

They isolated the infected system to control the impact of the incident beyond the currently affected assets and resources. This method implemented network segmentation to restrict the attacks ability to spread to other parts of the system

Gaps identified

-The containment phase lacked coordinated efforts which can lead to inconsistent containment effort of the blue team and the ransomware exploited vulnerabilities on endpoints which allowed the ransomware gain a foothold.

Recovery phase

The blue team attempted to restore the systems from the backup and clean the system from remaining ransomware. This process was to ensure that the system's integrity and security was up to standard.

Gaps noticed in the recovery phase

-The recovery took longer than expected due to inconsistency and outdated backup. This resulted in prolonged downtime and financial losses.

5.1 INTEGRATION OF RED TEAM TO IMPROVE RESPONSE

Integrating the red team into an organization's incident response (IR) plan can significantly enhance response capabilities. The red team simulates real-world attacks on a company's system and aim to identify vulnerabilities that could be exploited by malicious attacks

-Exercises of the red team to identify vulnerabilities and attacks

-Ethical hacking: the red team simulates attacks on the systems with the permission of the owners to identify vulnerabilities and test security measures

-Social Engineering skills: here the red team tries manipulating employees to reveal sensitive information, this process help gauge how employees adhere to security protocols

-Analyzing source codes of websites architecture and applications for vulnerabilities that could be exploited in an attack

Purple team

This is a team that combines the defensive and offensive security of both the red and the blue team. They simulate malicious attacks and penetration testing to identify security vulnerabilities and recommend remediation strategies for an organization's IT infrastructure (Sujatha *et al.*, 2023).

Ways the purple team can elevate incident response effectiveness

This allows an organization test their existing cyber defenses and capabilities in a low-risk environment

-The purple team elevates awareness among staffs to the risk of human vulnerabilities which may compromise the organization's security

-This strengthens the network security to detect targeted attacks and improve breakout time

-Real-time feedback loops

-Efficient use of resources

REFERENCES

Ahmad, W. *et al.* (2021) 'Cyber Security in IoT-Based Cloud Computing: A Comprehensive survey,' *Electronics*, 11(1), p. 16.

Capuano, N. *et al.* (2022) 'Explainable Artificial Intelligence in CyberSecurity: a survey,' *IEEE Access*, 10, pp. 93575–93600.

Liu, M. *et al.* (2024b) 'Enhancing Cyber-Resiliency of DER-Based smart Grid: a survey,' *IEEE Transactions on Smart Grid*, 15(5), pp. 4998–5030.

Mazhar, T. *et al.* (2023) 'Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods,' *Future Internet*, 15(2), p. 83.

Sun, N. *et al.* (2023) 'Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A survey and New Perspectives,' *IEEE Communications Surveys & Tutorials*, 25(3), pp. 1748–1774.