DIGITAL EMPOWERMENT NETWORK

INTERNSHIP REPORT

WEEK#03

PRESENTED BY ALIZA JAVED
CID DEN10161

CONTENTS

ABOUT THE COMPANY

At Digital Empowerment Network, we are dedicated to empowering Pakistan's university students through a wide range of initiatives that foster leadership, academic growth, and technical expertise. By bridging the digital divide with workshops, coding camps, and hackathons, we equip students with essential skills to thrive in the modern workforce. Our commitment to education extends beyond the classroom, as we reinvest proceeds from our revenue-generating partnerships into impactful programs and charitable initiatives, providing resources and support to underserved communities. We believe in the power of education to create well-rounded individuals who can drive innovation and make a positive impact on society..

DEVELOPING INCIDENT RESPONSE PLAN

1.Objective:

Create a plan for responding to security incidents.

2.Description:

Develop a structured approach for responding to and managing security incidents. Ensure the plan minimizes damage and facilitates quick recovery.

3.Key Steps:

- Identifying potential security incidents and scenarios.
- Defining roles and responsibilities for the response team.
- Developing step-by-step response procedures.
- Conducting training and simulation exercises.
- Reviewing and updating the plan regularly.

OVERVIEW

This report outlines the development and implementation of an Incident Response Plan (IRP) at Digital Empowerment Network as part of ongoing cybersecurity initiatives. The IRP is essential for effectively managing and mitigating security incidents, ensuring the organization can respond promptly to potential threats.

Key components of the IRP include identifying possible incidents, defining roles and responsibilities within the response team, and establishing clear procedures for detection, containment, eradication, and recovery. The report also emphasizes the importance of continuous training and regular updates to the plan to adapt to new security challenges.

Additionally, the report references industry standards, such as NIST and ISO, which guide the creation of effective IRPs, aligning the organization with best practices in cybersecurity management. By implementing this structured approach, Digital Empowerment Network aims to enhance its security posture, safeguard sensitive data, and maintain operational continuity.

INTRODUCTION TO INCIDENT RESPONSE PLAN (IRP)

In today's digital world, organizations face numerous security threats, such as data breaches and malware attacks. To manage these risks, businesses need an Incident Response Plan (IRP). An IRP provides a structured approach to quickly and effectively handle security incidents, minimizing damage and recovery time.

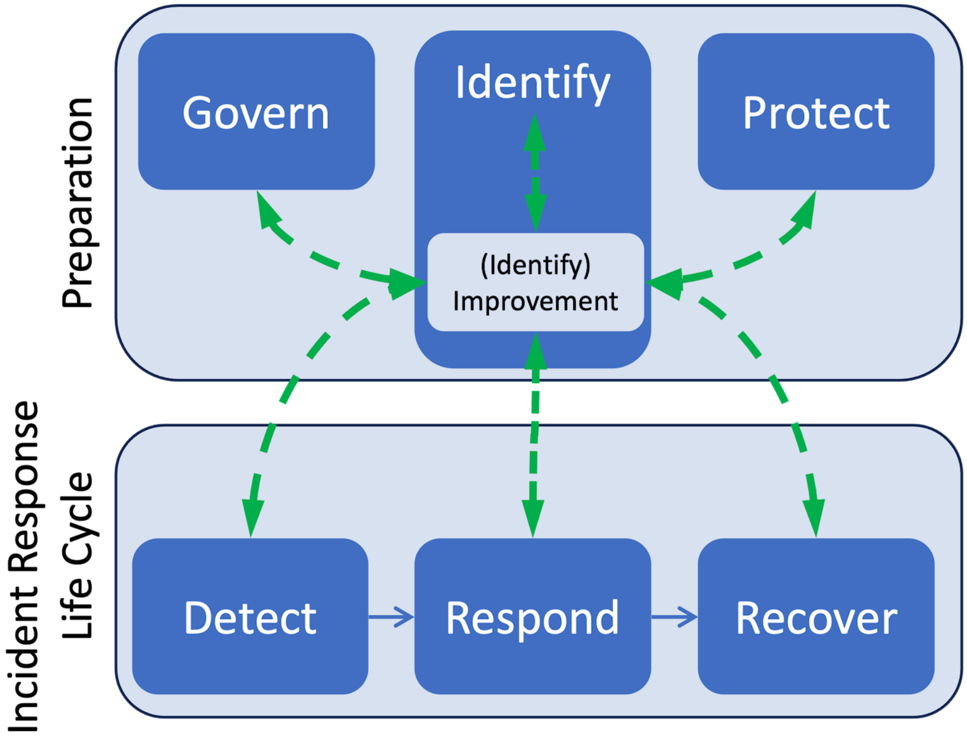
A well-designed IRP includes key components such as identifying potential incidents, assigning roles to the response team, and outlining procedures for detecting, containing, eradicating, and recovering from threats. Regular training and simulations ensure preparedness, and the plan should be continuously updated to adapt to evolving threats.

By implementing an IRP, organizations can protect sensitive data, maintain business continuity, and preserve trust with stakeholders.

INCIDENT RESPONSE PLAN LIFECYCLE

The incident response plan lifecycle contain the following components:

1. Preparation - Develop a policy approved by management, identify critical data and systems, single points of failure, train staff on incident response, implement an incident response team, practice incident identification (first response), identify roles and responsibilities, and plan the coordination of communication between stakeholders.
2. Detection and Analysis - Monitor all possible attack vectors, analyze incidents using known data and threat intelligence, prioritize incident documentation, and standardize incident documentation.
3. Containment, Eradication, and Recovery - Gather evidence, choose an appropriate containment strategy, identify the attacker, and isolate the attack.
4. Post-Incident Activity - Identify evidence that may need to be retained, document lessons learned.



INDUSTRY STANDARDS

Incident Response Plans (IRP) are structured approaches used by organizations to identify, manage, and recover from security incidents effectively. Several industry standards and frameworks guide the development and execution of these plans to ensure best practices are followed. Here are some of the most prominent standards in detail:

1. **NIST Special Publication 800-61 Rev. 2** provides a comprehensive guide for incident response, detailing each stage from preparation to post-incident analysis. It emphasizes establishing an incident response team, performing detection and analysis through monitoring, and managing containment, eradication, and recovery. The framework is widely used by organizations due to its flexibility and applicability, offering guidelines on creating effective incident response plans and learning from each incident to continuously improve the organization's security posture.
2. **ISO/IEC 27035** is an international standard that offers a systematic approach to information security incident management. It outlines the full incident response lifecycle, starting with planning and preparation, followed by incident detection, assessment, and response. The standard is focused on ensuring that organizations are prepared to handle incidents through predefined processes while emphasizing continuous learning and improvement after each incident. ISO/IEC 27035 is recognized globally for its structured and clear framework, making it valuable for organizations seeking an internationally recognized standard.
3. **SANS Institute's Incident Handler's Handbook** is a practical guide that outlines clear steps for managing security incidents, from preparation to post-incident analysis. It breaks down the process into actionable phases like identification, containment, eradication, and recovery. The handbook is particularly suited for incident handlers and cybersecurity professionals, offering detailed guidance on how to handle incidents in real-world situations while ensuring systems are restored securely and future incidents are prevented.
4. **CIS Control 17:** Incident Response Management is part of the broader CIS Controls and focuses on establishing an organization's capability to detect, respond to, and recover from cybersecurity incidents. It emphasizes preparation, detection through automated systems, containment, eradication, recovery, and learning from incidents

to update response procedures. This control is particularly beneficial for organizations that aim to align their incident response plans with a larger set of security best practices provided by the CIS framework.

5. **NIST Cybersecurity Framework (CSF)** provides a high-level overview of cybersecurity risk management, including incident response as one of its core components. It breaks the process into five functions: Identify, Protect, Detect, Respond, and Recover. While not exclusively focused on incident response, the NIST CSF is highly adaptable, allowing organizations to tailor their cybersecurity and incident response strategies to their specific needs, making it widely applicable across various industries and organizational sizes.

INCIDENT RESPONSE PLAN

Executive Summary:

- **Date:** September 23, 2024
- **System:** Apache Web Server
- **Host IP:** 192.168.56.1
- **Reported by:** ModSecurity Web Application Firewall
- **Event Type:** Web Application Attack Detection
- **Affected Systems:** Public-facing web server with IP 192.168.56.1
- **Incident Severity:** Medium
- **Status:** Resolved

1. Detection

ModSecurity logs revealed multiple suspicious activities indicating attempts to exploit the Apache web server. These activities, such as SQL injection and cross-site scripting (XSS), were flagged by the firewall's pre-configured detection rules. Continuous monitoring of the logs ensured early identification of these attack attempts. Alerts were promptly configured to notify the security team of these potentially harmful actions, reducing response time and preventing further exploitation.

2. Analysis

The first step in analyzing the incident involved verifying the accuracy of the alerts generated by ModSecurity. This was essential to rule out false positives and ensure that the detected anomalies were real attack attempts. A thorough impact assessment was conducted to determine if any sensitive data had been compromised or if the web service had been affected. Additionally, the source IP (192.168.56.1) and associated network traffic were investigated to identify the attack's origin and scope.

3. Containment

To prevent the attack from escalating, containment measures were immediately implemented. The affected server was isolated by updating the firewall rules, blocking all incoming traffic from suspicious IP addresses identified during the analysis. Access to vulnerable web server directories was restricted, and security protocols were adjusted to reduce the server's exposure. These steps ensured that the attack could not spread to other systems within the network.

4. Eradication

Once containment was ensured, the next priority was to remove any malicious content that had been introduced during the attack. The server was thoroughly scanned, and any suspicious files or scripts left by the attackers were eliminated. Additionally, the Apache server and web application were updated to the latest versions, applying all necessary patches to resolve any existing vulnerabilities. This step ensured that the environment was secure from the same or similar threats moving forward.

5. Recovery

After eradicating the threat, the focus shifted to restoring the server to its fully operational state. The server was restored from verified clean backups, and all systems were tested to confirm their integrity. Monitoring was intensified post-recovery to track any unusual behavior or recurrence of malicious activities. This ensured the system's stability and that no lingering threats remained.

6. Post-Incident Review

A comprehensive review of the incident was conducted to better understand the attack, its origin, and its effectiveness. This analysis highlighted areas where the response could be improved and provided insights for refining the overall incident response strategy. Based on the findings, incident handling procedures were updated, and new defensive measures were added to bolster the system's security. Training sessions were conducted for the relevant teams to ensure they were aware of the updated response tactics and emerging threats.

INCIDENT RESPONSE ROLES AND RESPONSIBILITIES

Effective incident response involves various roles and responsibilities within an organization, including:

- **Incident Handlers**
  - Verify incidents and assess their impact.
  - Collect evidence and coordinate the response process.
  - Mitigate damage and restore normal operations.
- **Leadership**
  - Oversee incident response activities and make critical decisions.
  - Authorize actions such as service shutdowns if necessary.
- **Technology Professionals**
  - Address technical aspects of incident response, including securing systems and restoring functionality.
  - Collaborate with incident handlers to implement containment and eradication measures.
- **Legal Teams**
  - Ensure compliance with regulations during the incident.
  - Provide guidance on legal implications and communication strategies.
- **Public Affairs**
  - Manage communications with the media and public during high-visibility incidents.
  - Coordinate messaging to maintain the organization's reputation.
- **Human Resources**
  - Involved when incidents relate to employee actions, such as insider threats.
  - Handle any necessary personnel actions or investigations.
- **Third-Party Service Providers**
  - Support incident response efforts, especially in managed services (e.g., cloud or network infrastructure).
  - Clearly define roles and responsibilities in contracts to ensure effective collaboration.

CONCLUSION

In conclusion, the development and implementation of an Incident Response Plan (IRP) are essential for an organization's preparedness against security incidents. The structured approach outlined in this report enables effective detection, response, and recovery from cybersecurity threats. By clearly assigning roles and responsibilities, conducting regular training, and keeping procedures up-to-date, organizations can minimize damage and ensure business continuity during security breaches.

Adhering to established industry standards such as NIST, ISO, and CIS enhances incident response strategies, aligning them with best practices. This not only strengthens technical responses but also underscores the significance of learning from each incident to continuously improve the organization’s overall security posture.