Incident Response Plan

By Kershia Mukoro

Disclaimer: Names and specific details in this document have been changed to ensure privacy and confidentiality.

Contents

The Company Incident Response Plan (IRP)

1. Introduction

Purpose

This Incident Response Plan outlines the procedures and guidelines to effectively respond to security incidents. The objective is to minimize the impact of incidents through timely responses, ensuring business continuity and the protection of sensitive information.

Scope

This IRP applies to all security officers, other employees, and third-party services that interact with The Company's information systems and data.

2. Definition of a Security Incident

A security incident is an event that may lead to a breach of information security and includes, but is not limited to:

- Unauthorized access or attempts to access data or systems.
- Loss or theft of devices containing corporate data.
- Attacks on IT infrastructure such as malware infection, phishing, or denial-of-service attacks.
- Accidental data exposure or data leakage.
- Compromise of user credentials.

Severity Levels

Incidents are categorized by severity levels:

- **High Severity:** Likely to cause significant harm or disruption, or affects sensitive/confidential data.
- **Medium Severity:** Causes moderate disruption or risk, affecting internal systems without involving sensitive data.
- **Low Severity:** Minor impact, easily contained, and does not affect sensitive data or critical systems.

3. Incident Response Team (IRT)

Team Composition

- **IRT Leader:** Coordinates all activities of the IRT and makes high-level decisions.
- **Security Analysts:** Perform technical analysis, manage containment, eradication, and recovery tasks.
- **Communications Officer:** Handles all communications, internal and external.
- **Legal Advisor:** Manages compliance with legal requirements and assists with any legal implications.

Roles and Responsibilities

- **Before an Incident:** Engage in continuous monitoring, training, and preventive measures.
- **During an Incident:** Follow the IRP, manage the incident, and minimize damage.
- **After an Incident:** Conduct post-incident reviews, document lessons learned, and update the IRP as necessary.

4. Communication Plan

- **Initial Contact:** Notify the IRT Leader immediately upon discovery of an incident.
- **Internal Notification:** Use the designated communication platform (e.g., email, internal chat) to inform relevant internal teams.
- **External Communication:** Managed by the Communications Officer, who will coordinate with external entities like law enforcement, media, or affected clients as necessary.
- **Backup Contacts:** If primary contacts are unavailable, backup team members must be called. A contact list is maintained and regularly updated.

5. Incident Response Procedures

Common Threats and Responses

- **Data Breach:** Isolate affected systems, assess the scope of the breach, notify affected parties, and engage legal counsel.
- **Malware Infection:** Disconnect infected systems, analyze malware, clean or rebuild affected systems, and restore from backups.
- **Phishing Attacks:** Secure accounts affected, analyze phishing emails, block sender, and reinforce employee training.

Expanding Coverage

- Gradually expand the IRP to include less common scenarios, continuously updating the response strategies based on emerging threats.

6. Recovery Scenarios

- **System and Data Recovery:** Utilize backups to restore data and systems. Regularly test backup integrity and restoration processes.
- **Continuity of Operations:** Switch to alternative systems or manual processes if necessary to maintain critical operations.

7. Authorities and Reporting

- **Internal Reporting:** Report to the IRT, executive management, and relevant department heads.
- **External Reporting:** Comply with legal requirements for reporting incidents. In Colorado, USA, this includes notifying local law enforcement and potentially affected Colorado residents in cases of data breaches involving personal information.

8. Review and Maintenance

- **Regular Reviews:** Conduct annual reviews of the IRP to incorporate new technologies, threats, and business processes.
- **Continuous Improvement:** Implement improvements based on feedback from drills, actual incidents, and changes in the business environment.

9. Approval and Implementation

- **Approval:** The IRP must be approved by senior management.
- **Implementation:** All staff must be trained on their specific roles within the IRP. New employees receive training as part of their onboarding process.