Comprehensive Analysis and Remediation of a Compromised Debian Server - Phase 3

Guillermo J. Costa H.
December, 9, 2024
4Geeks Academy

Introduction

In an era where cybersecurity threats are increasingly sophisticated, having a robust Incident Response Plan (IRP) and a comprehensive Information Security Management System (ISMS) is paramount for organizations. This document outlines the design of an IRP based on NIST SP 800-61 guidelines and the development of an ISMS compliant with ISO 27001 standards. The goal is to ensure the organization is prepared to identify, contain, eradicate, and recover from security incidents while preventing future recurrences and protecting critical information assets.

Incident Response Plan and Implementation of an ISMS (ISO 27001)

Objective

To establish a structured approach to effectively respond to security incidents, minimize their impact, and prevent recurrence by adhering to NIST SP 800-61 guidelines.

Incident Response Lifecycle

1. **Preparation:**
    - Develop and maintain an incident response policy.
    - Assemble an incident response team (IRT) with defined roles and responsibilities.
    - Conduct regular training and simulations.
    - Maintain an inventory of critical assets and associated risks.
2. **Identification:**
    - Implement real-time monitoring systems for anomaly detection.
    - Establish criteria for defining an incident and its severity.
    - Use tools like SIEM to correlate logs and detect potential threats.
3. **Containment:**
    - Establish short-term containment (e.g., isolating affected systems).
    - Develop long-term containment strategies, such as implementing patches or reconfiguring firewalls.
    - Document containment actions and communicate with stakeholders.
4. **Eradication:**
    - Identify the root cause of the incident.
    - Remove malicious artifacts, such as malware or compromised credentials.
    - Validate that the threat has been completely eliminated.
5. **Recovery:**
    - Restore systems and data from verified backups.
    - Monitor systems for signs of recurring threats.
    - Conduct a post-incident review to identify lessons learned.

Response to Similar Incidents

For incidents like the previous attack:

- **Identification:** Use enhanced monitoring tools to detect unauthorized access attempts.
- **Containment:** Immediately isolate vulnerable services such as FTP and SSH.
- **Eradication:** Reconfigure services to remove vulnerabilities and implement MFA for critical accounts.
- **Recovery:** Reestablish services with updated configurations and passwords.
- **Prevention:** Regularly review and update access controls, perform penetration tests, and enforce strict password policies.

Data Protection Mechanisms

- **Regular Backups:**
  - Schedule daily incremental and weekly full backups.
  - Store backups in encrypted formats both on-site and off-site.
- **Data Encryption:**
  - Encrypt sensitive data at rest and in transit using AES-256.
  - Use HTTPS, VPNs, and secure file transfer protocols.
- **Access Controls:**
  - Enforce role-based access control (RBAC).
  - Implement MFA and secure credential management.

Implementation of an ISMS (ISO 27001)

Identification of Critical Assets

A comprehensive inventory of critical assets is vital to establish an effective Information Security Management System (ISMS). The following categories of assets have been identified for the compromised Debian server and its environment:

- **Hardware**:
  - Servers: Primary Debian server hosting critical applications.
  - Networking equipment: Routers, switches, and firewalls that ensure secure connectivity.
  - Backup devices: External drives and on-premise storage for redundancy.
- **Software**:
  - Operating systems: Debian and related configurations.
  - Applications: Web servers (e.g., Apache), databases, and custom software used for operations.
  - Monitoring tools: SIEM solutions for anomaly detection.
- **Data**:
  - Business-critical data: Customer information, operational documents, and reports.
  - Credentials: SSH keys, admin passwords, and API tokens.
  - Logs: System and application logs used for forensic analysis.

Initial Risk Assessment

The identified assets were evaluated for potential risks using a qualitative method. The risks were prioritized based on likelihood and impact, and the following table outlines key findings:

Asset	Risk	Likelihood	Impact	Priority
Debian server	Exploitation of known vulnerabilities	High	Critical	High
Credentials	Unauthorized access due to weak password policy	Medium	Critical	High
Backups	Data corruption during recovery	Low	High	Medium
Logs	Tampering or deletion of critical records	Medium	High	High

Initial Security Policies

To mitigate the identified risks, the following security policies were proposed:

1. **Asset Management**:
    - Maintain an updated inventory of all hardware and software assets.
    - Assign ownership and responsibilities for critical systems.
2. **Access Control**:
    - Enforce role-based access control (RBAC).
    - Require multi-factor authentication (MFA) for privileged accounts.
    - Implement a strict password management policy (e.g., regular updates and complexity requirements).
3. **Data Protection**:
    - Encrypt sensitive data using AES-256 for data at rest and TLS for data in transit.
    - Store logs in a secure, immutable format.
4. **Backup and Recovery**:
    - Perform daily incremental and weekly full backups.
    - Regularly test recovery procedures to ensure data integrity.

Initial Action Plan

The action plan outlines steps to address risks and establish foundational security practices for the ISMS:

1. **Month 1**: Conduct a detailed risk assessment for all assets.
2. **Month 2**: Implement role-based access control and enforce password policies.
3. **Month 3**: Deploy encryption measures and secure backup processes.
4. **Month 4**: Finalize documentation of policies and procedures for ISO 27001 certification readiness.

Conclusion

By implementing an IRP based on NIST SP 800-61 guidelines and developing an ISO 27001-compliant ISMS, the organization will enhance its ability to respond to and recover from security incidents effectively. These measures ensure the protection of critical information assets, strengthen the organization's overall security posture, and align operations with international standards for information security management. Regular reviews and updates will be integral to maintaining a resilient security framework.