Security risk assessment report

By Jovworie Tanshi

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You are a security analyst working for a social media organization. The organization recently experienced a major data breach, which compromised the safety of their customers' personal information, such as names and addresses. Your organization wants to implement strong network hardening practices that can be performed consistently to prevent attacks and breaches in the future.

After inspecting the organization's network, you discover four major vulnerabilities. The four vulnerabilities are as follows:

1. The organization's employees' share passwords.
2. The admin password for the database is set to the default.
3. The firewalls do not have rules in place to filter traffic coming in and out of the network.
4. Multifactor authentication (MFA) is not used.

If no action is taken to address these vulnerabilities, the organization is at risk of experiencing another data breach or other attacks in the future.

In this activity, you will write a security risk assessment to analyze the incident and explain what methods can be used to further secure the network.

Part 1: Select up to three hardening tools and methods to implement
1. Password Management Tools 2. Firewall Configuration and Monitoring 3. Multifactor Authentication (MFA) Implementation

Part 2: Explain your recommendations

1. **Password Management Tools**

Recommendation:
Implementing a password management tool is essential to address the issue of password sharing and weak password policies. These tools can generate, store, and manage strong, unique passwords for all employees, reducing the risk of compromised credentials.

Benefits:

- **Enhanced Security:** Ensures that all passwords are complex, unique, and stored securely, reducing the risk of unauthorized access.
- **User Convenience:** Simplifies the process of managing multiple passwords, encouraging employees to follow best practices without the hassle of remembering numerous credentials.
- **Audit and Compliance:** Many password management tools offer auditing features to track password usage and ensure compliance with security policies.

Example Tools:

- LastPass
- Dashlane
- 1Password

2. **Firewall Configuration and Monitoring**

Recommendation: Properly configuring firewalls and setting up continuous

monitoring are crucial steps in protecting the network from unauthorized access and malicious traffic. This involves establishing comprehensive firewall rules and regularly updating them to adapt to new threats.

Benefits:

- **Traffic Control:** Filters incoming and outgoing network traffic based on predefined security rules, preventing unauthorized access and data breaches.
- **Threat Detection:** Continuous monitoring helps in identifying and responding to suspicious activities in real-time, minimizing potential damage.
- **Network Segmentation:** Allows the creation of separate network segments to isolate critical systems and limit the impact of potential breaches.

Implementation Steps:

- Define and implement detailed firewall rules based on the organization's security requirements.
- Regularly review and update firewall configurations to adapt to new threats.
- Set up continuous monitoring and logging to detect and respond to suspicious activities promptly.

Example Tools:

- pfSense
- Cisco ASA
- Palo Alto Networks

3. Multifactor Authentication (MFA) Implementation

Recommendation: Implementing MFA adds an additional layer of security by requiring users to provide two or more verification factors to gain access to systems and applications. This greatly reduces the risk of unauthorized access due to compromised passwords.

Benefits:

- **Increased Security:** Even if a password is compromised, MFA adds an extra layer of protection, making it significantly harder for attackers to

gain access.

- **Compliance:** Helps meet regulatory requirements for securing sensitive data.