Security risk assessment report #1

Scenario

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. Multi Factor 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.

Part 1: Select up to three hardening tools and methods to implement

To mitigate the identified vulnerabilities and strengthen network security, the organization should implement the following security hardening measures:

1. **Enforcing Multi-Factor Authentication (MFA)**
2. **Implementing a Password Management System & Policy**
3. **Configuring and Regularly Auditing Firewall Rules**

1. Multi-Factor Authentication (MFA) Implementation

MFA adds an extra layer of security by requiring users to authenticate using more than one method before accessing systems. This can include a combination of passwords, biometric authentication (fingerprint or facial recognition), security tokens, or one-time passcodes.

2. Password Management System & Policy

A password management system will help enforce strong, unique passwords across the organization and eliminate the need for employees to manually store or share credentials. In addition, a formalized password policy should require:

- Minimum password length and complexity requirements
- Regular password changes and restrictions on password reuse
- Automatic lockout after multiple failed login attempts
- Strict rules prohibiting password sharing

3. Firewall Configuration & Ongoing Audits

A properly configured firewall is essential for filtering incoming and outgoing network traffic. The organization should:

- Establish firewall rules that block unauthorized access attempts
- Regularly audit firewall settings and update rules as threats evolve
- Implement an Intrusion Detection System (IDS) to monitor for suspicious activity

Part 2: Explain your recommendation(s)

1. Enforce Multi-Factor Authentication (MFA)

Requiring employees to verify their identity using multiple authentication methods will significantly reduce the risk of unauthorized access. Even if a password is compromised, an attacker would still need the second authentication factor to gain entry. This method also discourages password sharing, as MFA ensures that access is tied to an individual's credentials and devices.

2. Strengthen Password Security & Eliminate Shared Credentials

Implementing a password management system will prevent employees from sharing passwords while ensuring that passwords remain strong and unique. A comprehensive password policy will further enhance security by making brute-force attacks more difficult and preventing credential stuffing attacks. Lockout mechanisms will also limit the risk of repeated unauthorized access attempts.

3. Strengthen Network Traffic Controls with Firewall Policies

Firewalls serve as a frontline defense against unauthorized access. Establishing and maintaining **strict firewall rules** ensures that only legitimate traffic flows into and out of the network. Conducting **routine firewall audits** will allow administrators to refine security settings based on the latest threat intelligence. Additionally, integrating **Intrusion Detection Systems (IDS)** will enable real-time monitoring of network activity, helping identify and respond to threats quickly.

By addressing these security vulnerabilities, the organization can significantly reduce the likelihood of future data breaches, protect customer data, and strengthen overall security posture.