Security Risk Assessment Report

Security Risk Assessment Report
Organization: Social Media Organization
Analyst: Nazish Khalid

---

1. Incident Overview

The organization recently experienced a major data breach that compromised customers' personal information, including names and addresses. Upon investigation, four critical vulnerabilities were identified that could have contributed to the security incident. This assessment provides an analysis of these vulnerabilities and outlines mitigation strategies to strengthen the network against future attacks.

---

2. Identified Vulnerabilities and Risk Analysis

Vulnerability 1: Employees Share Passwords

Risk: Password sharing increases the likelihood of unauthorized access and makes it difficult to track accountability. If one password is compromised, multiple accounts may be at risk.

Mitigation Strategies:

- Implement **individual user accounts** with unique credentials.
- Enforce a **strict password policy** that includes complexity requirements and expiration periods.
- Conduct **regular security awareness training** to educate employees on password hygiene.

Vulnerability 2: Default Admin Password for the Database

Risk: Default passwords are easily guessable or available in online repositories, making it easy for attackers to gain unauthorized access to the database.

Mitigation Strategies:

- Immediately **change the default admin password** to a strong, unique passphrase.
- Enforce **role-based access control (RBAC)** to limit administrative privileges.
- Regularly audit credentials and change passwords if compromise is suspected.

Vulnerability 3: Lack of Firewall Rules for Traffic Filtering

Risk: Without properly configured firewall rules, malicious traffic can easily enter the network, increasing the risk of external attacks such as malware infections or unauthorized access.

Mitigation Strategies:

- Implement **strict firewall rules** to filter incoming and outgoing traffic based on security policies.
- Deploy **intrusion detection and prevention systems (IDS/IPS)** to monitor network traffic.
- Regularly **review and update firewall configurations** to address emerging threats.

Vulnerability 4: Absence of Multifactor Authentication (MFA)

Risk: Without MFA, compromised passwords can grant unauthorized access to sensitive systems. MFA adds an additional layer of protection by requiring a second verification factor.

Mitigation Strategies:

- Implement **MFA for all user accounts, especially those with administrative privileges**.
- Use **biometric authentication, security tokens, or one-time passcodes (OTP) for additional security**.
- Educate employees on the importance of MFA and provide training on how to use it.

---

3. Conclusion and Recommendations

The identified vulnerabilities present significant security risks that could lead to future data breaches if not addressed. By implementing the recommended security measures, the organization can significantly strengthen its network defenses and reduce the likelihood of cyberattacks.

Key Recommendations:

- Enforce strong authentication and password management policies.
- Secure administrative accounts by changing default credentials and limiting privileges.
- Implement robust firewall configurations to filter and monitor network traffic.
- Mandate multifactor authentication (MFA) to add an extra security layer.
- Conduct **regular security audits and penetration testing** to identify and address new vulnerabilities.

By taking these steps, the organization will enhance its security posture, protect customer data, and prevent future security incidents.

Prepared by: Nazish Khalid
Position: Security Analyst