Oksana Syvun

# Security Risk Assessment Report

**Disclaimer:**

This security risk assessment report is intended to showcase my skills and expertise in identifying potential security risks and vulnerabilities. The scenarios presented are fictional and created solely for the purpose of demonstration.

As the author, I affirm that the content of this report does not reflect any real-world security threats faced by any organization. Rather, it is a testament to my analytical abilities and understanding of security principles.

Potential employers are encouraged to review this report as evidence of my capabilities in conducting thorough security assessments and providing actionable recommendations.

## Executive Summary

This report aims to conduct a security risk assessment for the social media organization following a recent data breach that compromised the safety of customers' personal information, such as names and addresses. Four major vulnerabilities in the organization's network were identified, posing significant risks to data security and system integrity.

## Methodology

The following tools and methods were used to carry out this security risk assessment: Vulnerability Analysis: An automated vulnerability scanning tool was used to identify potential weaknesses in the organization's network infrastructure and systems.

Configuration Review: A thorough review of the security configurations of systems and network devices was conducted to identify potential deficiencies in the implementation of security measures. Interviews and Process Analysis: Interviews were conducted with organization staff, and processes and practices related to network security and password management were analyzed.

## Results of Risk Assessment

The risk assessment identified the following vulnerabilities and associated risks:

- Employees sharing passwords: This practice poses a significant risk as it compromises the integrity of access credentials and facilitates unauthorized access to the organization's systems and sensitive data.
- Default admin password for the database: The use of default passwords increases the risk of unauthorized access to the database, jeopardizing the confidentiality and availability of stored data.
- Lack of firewall rules to filter traffic: The absence of proper configurations in the firewalls exposes the organization to intrusion risks and malicious attacks, as effective measures to control and monitor network traffic are not being applied.
- Non-use of multifactor authentication (MFA): The absence of MFA makes user accounts more vulnerable to identity theft and credential theft, which could result in unauthorized access to the organization's systems and data.

## Recommendations

Based on the results of the risk assessment, the following recommendations are made:

- Implement a robust password policy: Establish a password policy that promotes the use of strong and unique passwords for each user account, as well as regular password changes.

Additionally, employees should be trained on the importance of not sharing passwords and using secure methods to store them.

- Update firewall security configurations: Configure and maintain appropriate traffic filtering rules in the firewalls to allow only necessary traffic and block unauthorized connections. Additionally, implement a real-time security monitoring solution to detect and respond to potential intrusions.
- Implement multifactor authentication (MFA): Enable multifactor authentication on all systems and services used by the organization. This will add an additional layer of security by requiring a second form of authentication, such as a code generated on a mobile device, in addition to the usual login credentials.

## Conclusions

The security risk assessment identified several vulnerabilities that pose significant risks to the social media organization. By implementing the proposed recommendations, the organization will be able to strengthen its security posture, reduce the risks of attacks, and protect the confidentiality, integrity, and availability of customer data. Regular audits and a proactive approach to security risk management are recommended to maintain a secure and reliable environment.