Security risk assessment report

CASE STUDY-01

You are a security analyst working for a social media organization, FinstaGram. 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.

Organization: FinstaGram
Prepared by: Navya Nagpal, Cybersecurity Analyst
Date: May 2, 2025

Objective

To assess potential cybersecurity risks to FinstaGram's application and recommend strategies to reduce exposure to threats.

Identified Risks

Risk ID	Risk Description	Likelihood	Impact	Risk Level
R001	**Unauthorized access**	**High**	**High**	**Crtical**
R002	**Weak admin passwords**	**Medium**	**High**	**High**
R002	**Outdated firewall rules**	**Medium**	**Medium**	**High**
R003	**MFA not used**	**High**	**Medium**	**High**

Hardening tools necessary

Three hardening tools that the social media organization should use to address the vulnerabilities found include:

1. Implementing MFA/2FA- Multifactor Authentication or Two Factor Authentication allows the user to use at least two ways to identify and verify their credentials before accessing the application. Some MFAs include usernames & passwords, fingerprint scans, face recognition, and one-time password(OTP) using verified e-mail or contact number.
2. Setting and enforcing strong password policies- This ensures the set of characters

chosen by a person to access the application is strong enough to prevent brute forcing it. This also focuses on using methods to salt and hash passwords.
3. Firewall maintenance- This includes checking and updating security configurations regularly to stay away from potential threats.

Recommendations
1. Use strong passwords adhering to the password policies, and conduct regular security audits. 2. Implementing MFA or 2FA for all admin accounts 3. Use HTTPS and encrypt all sensitive data in transit 4. Deploy IDS/IPS systems

Risk Monitoring & Review Plan
Review Frequency: Quarterly Responsible Team: InfoSec Department Next Review Date: September 2, 2025