**Security Risk Assessment Report**

**Executive Summary**

This report outlines the security vulnerabilities identified within the social media organization's network and proposes hardening methods to mitigate these risks and prevent future data breaches. The identified vulnerabilities include:

* Shared employee passwords
* Default admin password for the database
* Lack of firewall rules for traffic filtering
* Absence of multi-factor authentication (MFA)

**Part 1: Hardening Tools and Methods**

To address the identified vulnerabilities, the following hardening tools and methods are recommended for implementation:

1. **Multi-Factor Authentication (MFA):** This security measure requires users to verify their identity through two or more factors beyond a simple password. Examples of MFA factors include fingerprint scans, security tokens, one-time codes sent via SMS, or security questions.
2. **Strong Password Policies:** Enforcing robust password policies strengthens network security. These policies should dictate password complexity (length, character types), minimum update frequency, and disallow password reuse. Additionally, consider implementing account lockout mechanisms after a set number of failed login attempts.
3. **Firewall Configuration and Port Filtering:** Firewalls act as a security barrier between the internal network and external traffic. Regularly maintaining firewall rules is crucial. This involves establishing rules that filter incoming and outgoing traffic, blocking unauthorized access attempts, and closing unused ports to minimize the attack surface.

**Part 2: Effectiveness of Recommendations**

**Multi-Factor Authentication (MFA):**

MFA significantly enhances security by adding an extra layer of verification beyond a password. Even if a malicious actor compromises a user's password through phishing or other means, they would still be unable to gain access without the additional verification factor. This significantly reduces the risk of unauthorized access attempts like brute-force attacks. Additionally, MFA discourages password sharing, as having the password alone wouldn't grant access to the system.

**Strong Password Policies:**

Enforcing strong password policies minimizes the risk of successful brute-force attacks and unauthorized access through weak credentials. Complex passwords with a combination of uppercase and lowercase letters, numbers, and symbols are significantly harder to crack. Password managers can further strengthen security by eliminating password reuse and sharing practices.

**Firewall Configuration and Port Filtering:**

Regular firewall maintenance plays a critical role in network security. Implementing strict firewall rules filters incoming and outgoing traffic, blocking unauthorized attempts and unnecessary data flow through unused ports. This significantly reduces the attack surface and the likelihood of attackers exploiting vulnerabilities to gain access to the network.

**Conclusion**

By implementing these recommended hardening tools and methods, the social media organization can significantly improve its overall security posture. This multi-layered approach addresses the identified vulnerabilities and creates a more robust defense system against potential data breaches. It's crucial to continuously monitor and adapt security measures to stay ahead of evolving cyber threats.

**Recommendations**

In addition to the implemented hardening methods, consider incorporating the following:

* **Vulnerability Scanning and Patch Management:** Regularly scan systems and applications for vulnerabilities and promptly apply security patches to address them.
* **User Education and Training:** Educate employees on cybersecurity best practices, including password hygiene and phishing awareness, to minimize the risk of social engineering attacks.
* **Secure Remote Access:** Implement secure protocols like VPNs (Virtual Private Networks) for remote access, ensuring encrypted communication and access control.