Network Hardening Plan

Security Risk Assessment

The recent data breach in our social media organization has prompted a comprehensive review of our current network security measures. Four major vulnerabilities have been identified, and this document outlines a mitigation strategy for each.

Vulnerability: Employees' sharing passwords

- Recommended Hardening Technique: Implement a robust security awareness training program.
- Effectiveness: By training employees about the dangers of sharing passwords and the potential consequences, they are more likely to understand and adhere to security best practices. A well-educated workforce acts as the first line of defense against security threats.
- Implementation Frequency: Initial intensive training followed by quarterly refresher courses and updates on new security threats.

Vulnerability: The admin password for the database is set to the default

- Recommended Hardening Technique: Enforce a strong password policy and periodic password changes.
- Effectiveness: Strong, unique passwords significantly reduce the risk of unauthorized access. Periodic password changes prevent potential long-term undetected breaches.
- Implementation Frequency: Immediate change from default password. Enforce password changes every 60-90 days.

Vulnerability: Firewalls do not have rules in place to filter traffic

- Recommended Hardening Technique: Implement a well-defined firewall rule set and conduct regular audits.
- Effectiveness: Specific rules limit the traffic to only necessary and secure connections. Regular audits ensure that the rules are up-to-date and effective against evolving threats.
- Implementation Frequency: Immediate setup of a baseline rule set. Monthly rule set reviews and after any significant network changes.

Vulnerability: Absence of Multifactor Authentication (MFA)

- Recommended Hardening Technique: Implement MFA for all critical systems, especially admin access.
- Effectiveness: MFA requires two or more verification methods (something you know, something you have, or something you are). This multi-tiered approach significantly reduces the risk of unauthorized access. Even if a password is compromised, an attacker would still need the second factor to gain access, making breaches less likely.

- Implementation Frequency: Immediate implementation. Review MFA methods annually or as newer technologies emerge.

The hardening techniques recommended above target the identified vulnerabilities directly, emphasizing both immediate remediation and ongoing practices. Implementing these strategies will significantly decrease the organization's risk exposure and enhance our overall security posture.