Security Risk Assessment Report: Social Media Organization

Part 1: Hardening Tools and Methods to Implement

To address the vulnerabilities identified, the organization should consider implementing the following three hardening tools and methods:

Multi-Factor Authentication (MFA): MFA requires users to provide multiple forms of identification and verification before accessing an application or network. This can include a combination of fingerprint scans, ID cards, pin numbers, and passwords. By enforcing MFA, the organization can significantly reduce the risk of unauthorized access through brute force or related attacks. It also mitigates the potential for password sharing among employees. Regular enforcement of MFA is essential, particularly for employees with administrative privileges.

Strong Password Policies: Implementing and enforcing strong password policies is crucial to bolstering network security. Password policies should include rules regarding password length, complexity, and acceptable character sets. Additionally, it is recommended to include a disclaimer discouraging password sharing. Enforcing restrictions on unsuccessful login attempts, such as temporarily locking out users after a certain number of failed attempts, further enhances security.

Regular Firewall Maintenance: Performing regular maintenance of firewalls is essential to stay ahead of potential threats. This includes checking and updating security configurations on a periodic basis. Firewall rules should be updated promptly in response to security events, especially those that allow suspicious network traffic into the network. By maintaining and updating firewalls, the organization can effectively protect against various types of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

Part 2: Explanation of Recommendations

Enforcing multi-factor authentication (MFA) adds an additional layer of security to prevent unauthorized access to the network. By requiring users to provide multiple forms of identification, the organization significantly mitigates the risk of brute force attacks and reduces the likelihood of password sharing, especially among privileged users. Regular enforcement of MFA is crucial to maintaining a robust security posture.

Creating and enforcing a strong password policy within the organization enhances the overall security of the network. By implementing rules regarding password length, complexity, and prohibiting password sharing, the organization can effectively reduce the risk of unauthorized access. Regular enforcement and education on password security help reinforce the importance of strong passwords.

Regular firewall maintenance is essential to ensure the firewall remains up-to-date and capable of defending against emerging threats. By promptly updating security configurations and rules, the organization can protect against various DoS and DDoS attacks, maintaining the integrity and availability of the network.

By implementing these recommended hardening tools and methods, the organization can enhance its overall security posture, reduce vulnerabilities, and mitigate the risk of potential security incidents.