Security Risk Assessment Report – Network Hardening for Social Media Data Breach

Objective

This report assesses the causes and vulnerabilities that led to a recent data breach at a social media organization. It identifies weaknesses in authentication, network access control, and firewall management, and provides specific recommendations for network hardening methods and tools that can prevent similar breaches in the future.

Background

The organization suffered a major data breach that exposed customers' personal information such as names and addresses. A security review revealed the following four critical vulnerabilities:

1. Employees share passwords.
2. The admin password for the main database is still set to its default.
3. Firewalls lack inbound and outbound traffic filtering rules.
4. Multifactor authentication (MFA) is not implemented.

Each of these vulnerabilities creates an entry point for attackers and weakens the organization's overall security posture. Immediate and ongoing network hardening is required.

Step 3: Selected Hardening Tools and Methods

Hardening Tool/Method	Purpose	Frequency of Implementa
Firewall Configuration and Port Filtering	To control and restrict traffic entering and exiting the network. Helps detect and block unauthorized access attempts.	Continuous monitoring and monthly review of firewall rules.
Password Management Policy & Enforcement Tools	To prevent credential sharing and enforce password complexity and rotation. Tools such as LastPass Enterprise, Azure AD Password Protection, or Bitwarden Teams can be used.	Enforced continuously; reviewed quarterly.
Multifactor Authentication (MFA)	To provide an extra layer of security beyond passwords. MFA ensures users can access sensitive systems.	Always active; periodic policy review every six months.

Step 4: Recommendations and Justification

1. Enforce Strong Password Management and Policy Compliance

Shared and default passwords significantly reduce network integrity. Deploying a password management system and enforcing strong password rules (minimum 12 characters, complexity, expiration) prevents credential reuse. Tools like Azure AD Identity Protection can automatically flag weak or shared credentials.

Implementation Frequency: Continuous enforcement with quarterly compliance audits.

2. Enable and Enforce Multifactor Authentication (MFA)

MFA reduces the likelihood of unauthorized access even if passwords are compromised. It mitigates brute force, phishing, and credential-stuffing attacks by requiring an additional verification factor before access is granted.

Implementation Frequency: Mandatory organization-wide and permanent.

3. Configure Firewalls with Inbound and Outbound Filtering Rules

Unrestricted traffic allows attackers to exploit open ports and exfiltrate data. Applying firewall rules (allowing only necessary ports such as 80, 443, 22) and enabling stateful inspection improves visibility and control.

Implementation Frequency: Monthly review and after any network configuration change.

Proposed Network Hardening Workflow

1. Deploy centralized authentication (e.g., Active Directory or Okta).
2. Automate password rotation for administrative accounts.
3. Enable firewall logging and intrusion prevention (pfSense, Cisco ASA, Fortinet). 4.
Conduct monthly vulnerability scans.
5. Educate employees on secure credential practices and phishing awareness.

Conclusion

The data breach resulted from weak authentication controls and insufficient traffic filtering. Implementing firewall management, password hardening, and MFA directly addresses these vulnerabilities. Consistent monitoring and review will strengthen network security posture and protect sensitive user data from future breaches.

Cybersecurity Relevance

This project demonstrates key SOC analyst and network security engineer competencies: identifying vulnerabilities, mapping controls to threats, and implementing best practices aligned with the CIA Triad and NIST SP 800-53 standards.