REPORT
Post-Breach Security Recommendations

v1.0.1

Author:

Eldon Gabriel

June 12, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	👤 Author	Description of Changes
v1.0.0	02/15/2025	Eldon G.	Initial draft.
v1.0.1	06/12/2025	Eldon G.	Applied hierarchical structure, added a conclusion section.

SECTION 1.0: SECURITY VULNERABILITY ASSESSMENT

1.1 Project Description

As a Security Analyst for a social media organization, I was tasked with investigating and addressing security vulnerabilities following a major data breach. The breach compromised customers' personal information, including names and addresses, raising serious concerns about the company's network security posture.

1.2 Identified Vulnerabilities

During my assessment, I identified the following critical security weaknesses:

- **Password sharing** among employees increases the risk of credential theft.
- **The default admin password** on a database makes it an easy target.
- **No firewall traffic filtering**, leaving inbound and outbound traffic unmonitored.
- **Lack of Multi-Factor Authentication (MFA)** increases exposure to unauthorized access.

1.3 Recommended Hardening Tools & Techniques

The organization can implement the following three hardening tools and practices:

1. **Stronger Password Policies**
2. **Multi-Factor Authentication (MFA)**
3. **Firewall Maintenance**

These strategies address both technical controls and human behavior, creating a more resilient security environment.

1.4 Detailed Recommendations

Stronger Password Policies

- **Recommendation:** Enforce the use of complex passwords and require periodic updates.
- **Explanation:** Weak passwords are highly exploitable and commonly used in brute-force attacks.
- **Expected Outcome:** Decreased likelihood of credential-based attacks and improved access control.

Multi-Factor Authentication (MFA)

- **Recommendation:** Implement MFA across all systems, especially administrative access.
- **Explanation:** MFA reduces the risk of unauthorized access, even if passwords are compromised.
- **Expected Outcome:** Enhanced security posture and reduced impact of phishing or credential theft.

Firewall Maintenance

- **Recommendation:** Regularly audit firewall configurations and update access rules.
- **Explanation:** Well-maintained firewalls protect against unauthorized access and evolving threats.
- **Expected Outcome:** Stronger network perimeter defense and mitigation of DDoS or malware intrusion attempts.

SECTION 2.0: CONCLUSION

2.1 Key Takeaways

The post-breach assessment identified preventable vulnerabilities that directly contributed to the incident. A lack of basic security controls—such as MFA, proper password management, and firewall enforcement—left the organization exposed. Addressing these issues is vital to regaining customer trust and meeting compliance standards.

2.2 Next Steps and Risk Mitigation Strategy

To reduce future risk, the organization should:

- Immediately implement stronger access controls and MFA across all systems.
- Conduct employee awareness training to prevent credential sharing and social engineering attacks.
- Establish a quarterly firewall audit schedule and document all configuration changes.
- Monitor system logs and user behavior for unusual patterns using SIEM tools.

These recommendations will close critical security gaps, improve incident response readiness, and help the organization maintain a secure, compliant environment moving forward.