# Security risk assessment report

| Part 1: Select up to three hardening tools and methods to implement |
| --- |
| **Multi-Factor Authentication (MFA):** Implement MFA for all user accounts, especially administrative ones. This requires users to provide a second authentication factor in addition to their password, such as a code from a mobile app or a hardware token. This will significantly reduce the risk of unauthorized access even if a password is compromised.<br><br>**Robust Password Policies:** Enforce a strong password policy that requires users to create complex passwords with a minimum length, combination of uppercase/lowercase letters, numbers, and special characters. Additionally, enforce regular password changes (e.g., every 90 days) and prevent password reuse. This minimizes the effectiveness of brute-force attacks and enhances overall password security.<br><br>**Firewall Configuration and Management:** Implement a next-generation firewall (NGFW) that can perform deep packet inspection, intrusion prevention, and web application firewalling. This will provide comprehensive protection against a wider range of threats, including unauthorized access attempts, malicious traffic, and application-layer attacks. Regular firewall rule reviews and updates are essential to ensure ongoing protection. |

| Part 2: Explain your recommendations |
| --- |
| The recent security incident highlighted significant weaknesses in the company's security posture, primarily stemming from weak password management and inadequate firewall protection.<br><br>• **MFA:** The attacker's success in gaining unauthorized access through a brute-force attack demonstrates the inadequacy of relying solely on passwords. MFA provides an additional layer of security, making it exponentially more difficult for attackers to breach accounts even if |

they obtain a password.

- **Strong Password Policies:** The use of weak or default passwords is a common vulnerability that attackers exploit. Enforcing strong password policies and regular changes significantly reduces the risk of successful password-based attacks.
- **Firewall Upgrade:** The current firewall's inability to filter traffic effectively left the website vulnerable to malicious code injection and subsequent redirection. Upgrading to an NGFW with advanced capabilities will provide a robust defense against a wider array of threats, protecting the website and user data.

By implementing these recommendations, The client will significantly enhance its security posture, protect sensitive data, and mitigate the risk of future security breaches.