Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

1. Multifactor Authentication (MFA)
    ○ Addresses vulnerabilities: Employees sharing passwords; MFA not being used.
2. Firewall Configuration and Maintenance with Port Filtering
    ○ Addresses vulnerabilities: Firewalls lack rules to filter incoming/outgoing traffic.
3. Password Policies and Removal of Default Credentials
    ○ Addresses vulnerabilities: Default database administrator password; employees sharing passwords.

Part 2: Explain your recommendations
1. Multifactor Authentication (MFA) ● Why it is effective: MFA adds an extra layer of security by requiring users to verify their identity through multiple means (e.g., password + token or biometrics). This significantly reduces the risk of unauthorized access, even if passwords are compromised. It protects against brute-force attacks, phishing, and credential theft. ● Implementation frequency: Initially implemented once but should be maintained and audited regularly (e.g., semi-annually) to ensure all users are enrolled and authentication methods are up-to-date. 2. Firewall Configuration and Maintenance with Port Filtering ● Why it is effective: Port filtering blocks unauthorized communications (e.g., unnecessary open ports), preventing malware from communicating with external

servers or attackers from exploiting vulnerable services. Regular maintenance ensures rules adapt to emerging threats.
- Implementation frequency:
  Initial configuration should be done immediately, with quarterly rule reviews. Security incidents should trigger emergency updates.

3. Password Policies and Removal of Default Credentials

- Why it is effective:
  Password policies based on NIST guidelines (e.g., long, memorable passwords without forced rotation) reduce user burden while maintaining security. Removing default credentials eliminates common attack vectors (e.g., factory-set passwords).
- Implementation frequency:
  Default credentials must be removed immediately. Password policies should be enforced continuously (real-time validation) and reviewed annually.

How These Practices Prevent Future Breaches

- MFA and password policies make unauthorized access significantly harder.
- Port filtering reduces entry points for attackers.
- Together, these measures create layered defenses (defense-in-depth), making the network more resilient to attacks.

These recommendations align with industry best practices and the provided hardening tools documentation. Implementing them consistently will help prevent future data breaches and protect critical assets.