Security risk assessment report

You are a security analyst working for a social media organization. The organization recently experienced a major data breach, which compromised the safety of their customers' personal information, such as names and addresses. Your organization wants to implement strong network hardening practices that can be performed consistently to prevent attacks and breaches in the future.

After inspecting the organization's network, you discover four major vulnerabilities. The four vulnerabilities are as follows:

The organization's employees' share passwords.

The admin password for the database is set to the default.

The firewalls do not have rules in place to filter traffic coming in and out of the network.

Multifactor authentication (MFA) is not used.

If no action is taken to address these vulnerabilities, the organization is at risk of experiencing another data breach or other attacks in the future.

Part 1: Select up to three hardening tools and methods to implement
For the scenario above, I recommend the following 3 hardening tools: 1. Multifactor Authorization(MFA) 2. Revised baseline configuration requiring that passwords are not shared and no password for any asset can be set to default, and firewall maintenance, as well as frequent patch updates. 3. Port filtering

Part 2: Explain your recommendations

To address MFA not being used, using MFA is highly recommended for the security of the company as it will make sure that only authorized users have access to a given company asset. Implement ideally every 6 months.

A fully revised baseline configuration is essential as it ensures that the security team of a firm strictly complies to the requirements leading to a more secure corporation. Revise regularly each time the security team discovers a potential attack surface.

Port filtering is another way to decrease the possibility of security vulnerability as it ensures that the ports that are not needed are disallowed and the ports that are needed are allowed. Filter ports every time a new network connection is introduced.