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:

1. The organization's employees' share passwords.
2. The admin password for the database is set to the default.
3. The firewalls do not have rules in place to filter traffic coming in and out of the network.
4. Multi-Factor 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.

In this activity, you will write a security risk assessment to analyze the incident and explain what methods can be used to further secure the network.

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

1. Password policies
2. Multi-Factor authentication
3. Regular firewall maintenance

Password policies are guidelines set by the organization on how complex a password should be. They might be at least a specified length or must contain certain special characters. In addition, other rules can be implemented in place, such as kicking the user off the network after several unsuccessful password attempts.

Multi-factor authentication requires the user to add a second verification method in order to best ensure the user is legitimate. These can include a fingerprint scan, email verification, or a special PIN.

Lastly, regular firewall maintenance updating security configurations will prevent any vulnerabilities from being exploited by malicious threat actors.

Part 2: Explain your recommendations

The reason I am suggesting the implementation of password policies is to prevent any brute force attacks that involve guessing passwords. By setting complicated passwords that will be changed often, potential threats will be discouraged from trying to organize any attacks against this company.

A multi-factor authentication method is also suggested. In the scenario a malicious threat actor obtains the password to this social media organization, they still must verify themselves. Implementing this on top of the password policies will ensure absolute security of valuable and sensitive information and data.

The last issue that should be addressed are the firewalls. Currently, they don't do anything for the network, so firewall maintenance should be implemented to put them into use. With these firewalls in place, the organization's attack surface should be reduced.