Security risk assessment report

Scenario

Review the following scenario. Then complete the step-by-step instructions.

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. 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.

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
Password policies, Firewall maintenance, and Encryption using the latest standards

Part 2: Explain your recommendations
Implementing strong Password policies such as increasing the minimum length of required passwords, requiring the password to include numbers and special symbols make it harder for brute force attacks and for password guessing. It's recommended to have a password policy where passwords cannot be shared and that MFA should be used. Implementing Firewall maintenance and regularly updating firewall rules will help block unwanted visits from employees to unsecure sites and will block the

outside internet from access to the internal network. Also, updating the firewall's port filtering rules will help block unused ports to add an extra layer of security.

Finally, Implementing Encryption using the latest standards will protect the data even when the network is compromised as the threat actor won't be able to understand the leaked data.