Case Study:

Analysis of Network Hardening - Creating a Security Risk Assessment Report

Scenario:

The social media organization you work for as a Security Analyst 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.

Write a security risk assessment to analyze the incident and explain what methods can be used to further secure the network.

Security Risk Assessment Report

Network Hardening Tools and Methods to Implement
1. Implementing multi-factor authentication (MFA) - MFA requires users to use at least two ways to identify and authenticate their credentials before accessing an application. Some MFA methods include fingerprint scans, ID cards, pin numbers, and passwords. - It is recommended to enforce multi-factor authentication (MFA) because it will reduce the risk of a malicious threat actor accessing the network through techniques such as brute force, dictionary attacks and more. Furthermore, MFA will also make password sharing difficult for employees within the organization, as well as, address the vulnerability of the admin password set to default. 2. Setting and enforcing strong password policies - Password policies can be refined to include rules such as acceptable characters, password length and a disclaimer to discourage password sharing. They can also include rules surrounding unsuccessful login attempts, for example the user losing access to the network after a certain number of unsuccessful attempts. - It is recommended to set and enforce strong password policies within the organization to add a layer of difficulty for malicious threat actors to access the network and increase user security. 3. Performing firewall maintenance regularly - Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. - It is recommended to perform firewall maintenance regularly and update rules whenever a security event occurs simply because it is good security practice to do so.