Security risk assessment report

Data Breach on social media organisation

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

3 hardening tools and methods the organisation can use to mitigate the vulnerabilities found:

- Creating and enforcing robust password policies
- Using Multi Factor Authentication
- Conducting penetration testing (addresses firewall vulnerability)

Part 2: Explain your recommendations

Robust password policies will discourage password sharing, increase password complexity and include additional logging in SIEM for suspicious login attempts. This will mitigate brute force attacks.

MFA will add to the identification process granting only legitimate users access to the company's systems. Can be either a OTP sent to a trusted device, biometrics or ID cards. This will also make it difficult to share passwords as there is another step in the identification process before granting access.

Conducting Penetration testing will identify threats and vulnerabilities to the companies systems such as their website, firewalls, servers and endpoints. Network admins can review their firewall rules, and add suspicious traffic sources to their blacklist. They can disable unused ports and implement port filtering to regulate their network traffic. This measure can mitigate DoS and DDoS attacks.