Security risk assessment report

5th February 2025

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.

Jefferson Yankson

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
To prevent user data breaches, some security hardening operations the organization can perform are: • Implementing Multi-Factor Authentication (MFA) or 2FA • Setting Password Policies • Configuring Firewalls to Filter Unwanted Network Communications

Part 2: Explain your recommendations
1. Implementing Multi-Factor Authentication (MFA) Multi-factor authentication (MFA) is a security control that requires an extra step of authentication, allowing users to confirm their identity through various processes. Users can verify their identity through methods such as: • Biometrics • A special question • A one-time password (OTP) This additional security measure ensures that only authorized users can access sensitive information, significantly reducing the risk of data breaches. 2. Setting Password Policies The organization must set robust password policies and encourage users to practice good security habits. These policies should enforce the following standards: Password complexity: Require passwords to include a mix of uppercase, lowercase, numbers, and special characters.

Jefferson Yankson

Regular updates: Passwords should be changed at regular intervals to minimize the risks associated with stale credentials.

Prevention of password reuse: Users should not be allowed to reuse old passwords, reducing the likelihood of passwords being compromised across multiple accounts.

By ensuring employees follow these guidelines, the organization can maintain a strong security posture and protect user data from being easily exploited.

3. Configuring Firewalls to Filter Incoming and Outgoing Traffic

Network administrators must ensure that firewalls are properly configured to filter unwanted traffic. This includes:

Monitoring incoming traffic to detect any suspicious IP packets from untrusted sources.

Block unapproved connections to prevent unauthorized access to internal systems.

Configuring firewalls to filter traffic ensures that malicious actors cannot easily exploit vulnerabilities, limits potential attack surfaces, and helps prevent Denial of Service (DoS) attacks.