Security risk assessment report

By: Krithik Tamilselvan

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

Some possible solutions may be:

- Enable 2-Factor Authentication
- Reconfiguring the Firewall
- Have Employees update their passwords monthly

Part 2: Explain your recommendations

By having a multi-factor authentication (MFA) system there is a better form of protection than a one-time log-in. With the implementation of the MFA, there will be less likelihood of someone entering through brute force or another related attack. Additionally, with the MFA there is a lesser chance for people to log in when only knowing the password, as they would need to know another login.

Another addition that would help security hardening would be updating the firewall rules and restrictions. If the administration can regulate their rules there can be an up-to-date standard. A good firewall blocks incoming threats if the IDS or IPS is unable to detect or deflect.

When mandating monthly password changes, this organization can ensure that passwords won't be viewed or taken by attackers with brute force. Additionally, employees should be encouraged to create strong, unique passwords and use password management tools to maintain them securely.