Security risk assessment report

Scenario

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.

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

Some hardening tool that the organization can use to prevent this kind of attacks are:

1. Implementing multi factor authentication (MFA)
2. Performing Firewall maintenance routinely
3. Implementing Network access privileges
4. Setting strong password policies

MFA is a security measure which requires a user to verify their identity in two or more ways. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more.

Firewall maintenance consists in checking and updating security configurations regularly to stay ahead of potential threats.

Network access privileges involves permitting, limiting, and/or blocking access privileges to network assets for people, roles, groups, IP addresses, MAC addresses, etc.

Password policies are a set of rules about the creation and use of passwords. These policies can include rules regarding minimum length, complexity and composition, acceptable characters and messages warning about password sharing. Furthermore, they can include rules concerning unsuccessful login attempts and expiration dates.

Part 2: Explain your recommendations

With the implementation of MFA, the organization can be more protected against brute force attacks and similar security events, since the attacker would have to work harder to pass the multiple authentications. This tool can also reduce the likelihood of sharing the passwords, since the person would need to possess multiple additional forms of authentication besides a password. Essentially, MFA makes passwords less useful. All of this adds a necessary additional layer of security.

The company needs to check and maintain the firewalls security configurations regularly. These rules need to be up to date standard for allowed and denied traffic. All suspicious traffic must be included in the denied traffic list. Finally, Firewall rules should be updated in response to an event that allows abnormal network traffic into the network.

The access to the network can be further protected by implementing network access privileges. The access to the data can be only permitted to certain roles or people and the unknown IPs can be blocked. This reduces the risk of unauthorized users and outside traffic from accessing the internal network.

Finally, the privileges should be revisited and updated after a brute force attack.

Writing a strong password policy and enforcing it will make it harder for malicious actors to access the network. Due to the nature of a brute force attack, after some login attempts, the attacker couldn`t enter the network. Moreover, increasing password complexity and not allowing password sharing also help stall malicious actors.