Security risk assessment report

By Jason Ash, Security Analyst at Pretend Social Media Company, Inc.

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 organization's employees' share passwords.
- The admin password for the database is set to the default.
- The firewalls do not have rules in place to filter traffic coming in and out of the network.
- Multi-factor authentication (MFA) is not used.

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

The admin password to the database must be changed regularly and follow the strong password guidelines in company policy (see updated policy at the end of this document). The database admin password must be unique and not be reused for any other logins within or outside of the company. It must not be written down, and if written down, then it must be stored in the company's on-site safe only accessible by VP or higher company officers.

The firewall needs to disable unused ports and filter packets based on the information in packet headers. Firewall configurations need to be checked regularly to prevent evolving threats.

Two-factor (2FA) or multi-factor authentication (MFA) need to be implemented.

The password policy has been updated to be strict and disallow password sharing. Any employee that engages in password sharing outside of express permission from the Director of IT or higher level will be disciplined up to and including termination.

Network access privileges must be implemented based on someones roles, and these will be further subdivided based on IP and MAC addresses.

Part 2: Explain your recommendations

Changing the password to the database from the default prevents anyone with knowledge of the default password including the vendor and manufacturer or previous employees from accessing the database. Moreover, it prevents brute-force and dictionary attacks. Having unique passwords prevents a malicious actor from accessing other accounts with that same password. Changing a password at regular intervals (for example, every 72 or 90 days) and upon an employee who has knowledge of that password no longer being employed by the company prevents unauthorized logins.

Only ports that are needed should be allowed, and any unused ports should be closed or disabled. This protects against port vulnerabilities and reduces the attack surface.

Packet filtering allows only trusted packets to leave the network and disallows packets from suspicious sources.

Multi-factor authentication combines the security principle of combining something someone knows, such as their password, with something they have, such as a DUO authenticator on a company-approved smartphone.

Updated Password Policy:
Password Requirements:

- A minimum of 15 characters in length
- Must contain at least one symbol and one number
- Cannot match in whole or in part any of the employee's three previous passwords
- Cannot contain more than three repeated characters in a row
- Cannot be a single word in any language found in their respective dictionaries.
- Password sharing with other employees or individuals outside of the organization will be strictly forbidden

A message reminding employees to change their password will be displayed 72 days after they previously changed their password. Employees must change their password by the 90th day after they last changed their password. Failure to comply will result in employees getting locked out of the system until IT resets their password and makes the employee change it. Password sharing will be strictly forbidden. Disciplinary action will follow anyone violating this policy up to and including termination.

Passwords serve as the first line of authentication for users, but DUO 2FA will also be required going forward which provides an extra layer of security by making it difficult to impossible for unauthorized users to log in with a stolen password without the second factor code generated by the DUO app.