Security risk assessment report

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

Listed below are the vulnerabilities in the company/system that allow for problematic securities issues. Highlighted in red are the hardening tools selected for each of the vulnerabilities.

1. The organization's employees' share passwords: install a MFA (multi-factor authorization) verification system to limit sharing passwords and ensure that each employee has their own, distinct login information that cannot be copied by another employee – no matter how innocent the purpose may be. Reset passwords and create and implement a password updating policy.
2. The admin password for the database is set to the default: change the default password so that it is not the admin password and change the admin password
3. The firewalls do not have rules in place to filter traffic coming in and out of the network: establish a Next Generation Firewall (NGFW) which would limit certain ports entering the network and could inspect data packets for potential threats. Any firewall performing port filtering would benefit the network. If NGFW is not feasible, then any firewall would be better than none.
4. Multifactor authentication (MFA) is not used: install a MFA (multi-factor authorization) verification system to limit sharing passwords and ensure that each employee has their own, distinct login information that cannot be copied by another employee – no matter how innocent the purpose may be. Reset passwords and create and implement a password updating policy.

Part 2: Explain your recommendations

At this time, implementing a firewall is recommended to help the overall security of the organization. Establishing a firewall will mean updating and monitoring the firewall at regular intervals. A stateless firewall provides the least amount of protection with a stateful firewall providing a higher level of security with a NGFW providing the highest level of security.

In addition to a firewall, incorporating MFA would significantly reduce the ability for a threat actor to gain access to logins and systems. This as well as implementing password expirations, including regularly updating admin passwords, would assist in the security for this company.