Security risk assessment report

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

Three hardening tools that should be implemented by the company are stricter password policies, firewall setup and maintenance, and multi-factor authentication.

Part 2: Explain your recommendations

One of the most glaring vulnerabilities of the network are the password policies. It has been found that employees are sharing passwords and the administrator's password is set to the default. This makes the administrator account especially susceptible to a brute force attack. Stricter password policies need to be put in place to strengthen security posture and ensure that another data breach does not occur. Refining password policies to include rules regarding password length, acceptable and required characters, and a disclaimer to discourage employees from sharing their passwords will improve security posture. Additionally, implementing rules surrounding unsuccessful login attempts will help prevent brute force attacks. For example, preventing the user from making a login attempt for one minute after 5 consecutive unsuccessful login attempts will make brute force and other attacks increasingly difficult and less efficient.

Secondly, the firewalls that are in place do not have any rules in place to filter out any traffic coming in or out of the network. This presents a great security risk since a malicious actor can easily gain access to the network without having to worry about being blocked by a firewall. Both configuring the firewalls to filter out suspicious traffic and then performing regular firewall maintenance to check and update these configurations will greatly improve overall security posture.

Finally, introducing multi-factor authentication (MFA) into the authentication process will improve security posture. Currently, the lackluster password policies in combination with the lack of MFA makes the network very susceptible to brute force or other attacks. By introducing MFA, even if an attacker guesses the correct password with brute force, they would still need to go through additional authentication to gain access. Implementing MFA in addition to the aforementioned password policy improvements will greatly improve security posture and help prevent any future data breaches.