Security Risk Assessment Report

Three hardening tools and methods to implement

Three security hardening tools and methods the organization can implement to improve their overall security posture and address the current vulnerabilities found are:

1. Multifactor authentication (MFA).
2. Creating and enforcing password policies.
3. Performing regular firewall maintenance, including port filtering.

Firstly, MFA requires authorized users to provide multiple forms of authentication to verify their identity before receiving authorized access. Additional MFA forms range from, biometrics, ID cards, one-time passwords (OTP), to time-based one-time passwords (TOTP).

In this case, password policies can be created with rules that meet the current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters). A disclaimer should also be added to discourage password sharing. Additionally, passwords should be updated at set times regularly and rules should be implements to restrict access to systems and networks after a number of unsuccessful login attempts.

Finally, the organization's firewall includes, reviewing and updating its security configurations to stay ahead of potential threats, and port filtering to disallow unused ports and to limit unnecessary and unwanted communications.

Explanation of recommendations

Multifactor authentication reduces the likelihood of unauthorized personnel accessing restricted information such as users' PII/SPII. MFA also reduces the likelihood of malicious actors gaining unauthorized access to the network through a brute-force or related attack. In relation to password sharing, MFA acts as a preventative measure, making this unsecure act more difficult. Identifying and verifying authorized credentials is especially critical among personnel with administrator level privileges on the network, as PoLP should be enforced. For these mentioned reasons, MFA should be regularly enforced.

Currently, there are no password policies in place. Implementing these necessary policies to increase the complexity and variation of passwords, and limit password attempts, would greatly reduce the likelihood of malicious actors conducting brute-force attacks to gain entry to the organization's systems by making it increasingly challenging. Additionally, password sharing must be discouraged, as this unsecure act that —

— increases the likelihood of unauthorized access to sensitive information. The rules implemented in the password policy must be regularly enforced within the organization to boost user security and improve the organization’s security posture.

Firewall maintenance should be implemented and routinely carried out. Firewall baseline rules and configurations should also be updated whenever a security event occurs. Especially, events that allow suspicious traffic into the organization’s network. This can mitigate various DoS and DDoS attacks. Port filtering also reduces the organization’s attack surface.