COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

2.G: Does the WWS detect and block repeated unsuccessful login attempts?

Recommendation: Enable System Administrators notification after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an Administrator.

Why is this control important?

Attackers try to break into OT / IT systems by "guessing" an actual username and password login combination, by manually guessing an account's password, using a list of common passwords, or using a brute force technique. The attacker submits combinations of usernames and passwords, generally using an automated, readily available password-cracking tool until the guess is correct. Blocking an attacker from future guesses after a specified number of incorrect guesses can stop these types of attacks. Without blocking login attempts, this attack will occur continuously until the attacker successfully cracks the password. A password cracker can run for hours, days, and weeks and eventually crack a password with brute force unless there is a policy that will stop it from happening.

Implementation Tips

Enable systems to automatically notify (e.g., by a computer-generated alert) security teams or the System Administrator after a specified number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in under 2 minutes).

Enable account lockout settings on applicable systems to prevent future login

Additional Guidance

- ✓ Depending on the version of Windows that a WWS uses, the System Administrator can use the Local Security Policy to restrict the number of login attempts. To access this feature, type "Local Security Policy" in the search box in the Start menu and click on the Local Security Policy App. Once the menu pane opens, click on "Account Policies" to adjust login attempts and lockout duration.
- ✓ If a WWS utilizes a Microsoft Domain with many systems and user accounts connected to a single domain, it can manage these settings using Group Policy Objects (GPOs). The System Administrator can enable the Account Lockout Policy settings in the following location in the Group Policy Management Console: Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy. The Microsoft Windows Security Policy Settings Reference linked below provides additional details.
- ✓ When implementing a login lockout threshold, ensure the account lockout threshold is set to an appropriate level based on the criticality of the system (generally between five to ten attempts). The selected level should provide leeway for operators to accurately input their credentials a few times but be robust enough to prevent most brute force attacks.

attempts for the suspicious account for a minimum time or until the account is re-enabled by the System Administrator.

Log and store the alert information for analysis. Use sound logging procedures - a log should capture the event source, date, username, timestamp, source addresses, destination addresses, and any other useful information that could assist in a forensic investigation.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See page 39, "Unsuccessful Logon Attempts" (control AC-7), for more information. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Center for Internet Security (CIS) Microsoft Windows Benchmark: This document describes how to implement preventative actions on Microsoft Windows-based systems. The section covering account lockout policy starts on page 50. Implementing detailed tracking is described on page 382.
https://www.cisecurity.org/benchmark/microsoft_windows_desktop

NIST Policy Template Guide: See Access Control Policy (6.a/6.b) Unsuccessful Logon Attempts. This policy details how many unsuccessful login attempts it takes to lock an account. *https://www.cisecurity.org/wp-content/uploads/2020/06/Access-Control-Policy.docx*

Microsoft Windows Security Policy Settings Reference: This page describes how to configure account lockout settings on Windows systems. *https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold*