Windows Kiosk Hardening Procedure

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, the Office of Information Security has established this configuration standard for a Windows standalone workstation that is consistent with an industry-accepted hardening standard. This procedure utilizes The Center for Internet Security CIS-CAT Tool. This standard should be implemented on all workstations that require PCI DSS compliance. It will be evaluated on an annual basis to ensure its adequacy and relevancy.

Procedure

1. Install Windows 10
2. Create Admin account
3. Update Windows 10 and configure windows settings
4. Run Windows 10 Debloater tool (Uninstall after finished)
    a. Uninstall bloatware apps
    b. Uninstall OneDrive
    c. Remove bloatware registry keys
    d. Disable telemetry
5. Clean up the file system (Remove unnecessary files/programs/registry entries)
6. Apply the Center for Internet Security CIS-CAT Windows 10 Remediation Kit using LGPO
7. Create Kiosk user
    a. Standard account
    b. No password
    c. Configure auto logon in registry

   d. Add schedule task with script to auto logon

   e. Logon to Kiosk user and configure start menu and taskbar

8. Install Chrome Browser
9. Add chrome (.adm) to group policy and configure it

   a. Configure group policy settings

   b. Logon to Kiosk user and configure favorites, home pages, and settings

10. Apply Group Policy settings to lock down Kiosk access to system tools, file system, start menu, and taskbar
11. Deny Kiosk user access to edge, command prompt, and PowerShell

Revision History

April 29, 2019 (Procedure Created)