5/16/2023

Secure Windows 10 Workstations from Data Loss & Malware Threats SOP

Purpose:

Implement security measures to protect the system, user data, and sensitive information from unauthorized access, malware infections, and potential data loss incidents.

Scope:

To establish a standardized approach for securing Windows 10 endpoint workstations, ensuring the confidentiality, integrity, and availability of data.

Responsibilities:

The IT department at Team Knonsense is responsible for the implementation, maintenance and review of this policy.

Prerequisites:

A. Administrative Access: Obtain administrative access to the Windows 10 system to implement security configurations and install necessary software.

B. Windows Firewall: Enable and configure the built-in Windows Firewall.

C. Backup Solution: Set up a reliable data backup solution, such as external drives, network-attached storage (NAS), or cloud-based backups. (See Backup and Restore user data, critical infrastructure configurations and hosted data SOP)

D. User Account Control (UAC): Configure User Account Control settings on the system.

Procedure:

It is important to conduct periodic security audits to assess the effectiveness of implemented security measures. Review logs, perform vulnerability scans, and analyze system configurations to identify and address any potential vulnerabilities or gaps.
Implementing security measures is an ongoing process that requires regular maintenance, updates, and user awareness.

1. Update Windows
   - Enable automatic updates or regularly check for updates manually.

2. Windows Virus and Threat Protection
   - Enable and perform regular scans to detect and remove any malware.

3. Enable and Configure Windows Firewall
   - Allow only necessary applications and services through the firewall.

4. Implement Strong Password Policies
   - Enforce strong password policies for user accounts and encourage users to create unique and complex passwords and periodically change them.

5. Perform Regular Data Backups
   - Refer to Backup and Restore user data, critical infrastructure configurations and hosted data SOP

6. Enable User Account Control (UAC)
   - Adjust the UAC settings to an appropriate level of security based on organizational needs.

7. Update Applications
   - Apply patches and updates provided by the software vendors to address security vulnerabilities.

References:

- https://www.thewindowsclub.com/windows-defender-security-center

Definitions:

- Malware - Malicious Software

Revision History:

5/16/2023 - Adrian Mundo