STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices Workgroup

Device Hardening Strategy

1. Purpose
   In an effort to further increase the overall security posture of the State of Montana, several agencies agreed to collaborate on a strategic goal of increasing security on end-user workstations. The agencies involved were: Department of Justice (Dawn Temple), Department of Corrections (Kim McIntyre), Department of Transportation (Lance Wetzel), Legislative Services (Darrin McLean), Office of Public Instruction (Jim Gietzen), and State Information Technology Services Division (Sean Rivera). The team met on a monthly basis between the March and August of 2015. The MT-ISAC Best Practices workgroup reviewed and updated this best practice from November 2015 to January 2016.

2. Research and Discussion
   Originally intended to assess the posture of antivirus, it became clear that budgetary constraints as a result of legislative decisions would prohibit any change or additional acquisition of an antimalware solution. The group decided to focus on studying best security practices that could be developed, implemented with no cost and minimal effort, and that would provide the greatest increase to security.

3. Policy
   Device hardening strategy applies to the following controls found within the Information Security Policy.
   a. Information Security Policy
      - Identify
        - 1.7, 1.7.6, 1.7.10, 1.7.12
      - Protect
        - 2.1.9, 2.6, 2.7, 2.7.1, 2.7.2, 2.9.2, 2.9.5.3, 2.9.5.8, 2.9.6, 2.10, 2.10.9, 2.11.6, 2.14.6, 2.15.6, 2.18.8, 2.19, 2.19.3, 2.19.4, 2.19.5
      - Detect
        - 3.1
      - Respond
      - Recover
   b. Information Security Policy – Appendix A
      - Access Control (AC)
        - AC-2 – Account Management
        - AC-3 – Access Enforcement
        - AC-6 – Least Privilege
      - Configuration Management (CM)
        - CM-2 – Baseline Configuration
        - CM-5 – Access Restrictions for Change
        - CM-7 – Least Functionality

- CM-11 – User Installed Software
- Identification and Authentication (IA)
  - IA-7 – Cryptographic Module Authentication
- Media Protection (MP)
  - MP-4 – Media Storage
  - MP-5 – Media Transport
- System and Service s Acquisition
  - SA-5 – Information System Documentation

- System and Information Integrity (SI)
  - SI-2 – Flaw Remediation (Patch Management)
  - SI-3 – Malicious Code Protection
  - SI-4 – Information System Monitoring
  - SI-7 – Software, Firmware, and Information Integrity
  - SI-16 – Memory Protection

4. Recommended Best-Practices to be Adopted as Standard Configuration

   a. Workstation Configuration (Enterprise Information Security Policy – 1.7, 2.6, 2.9.5.3, 2.10, 2.11.6, 2.19, 3.1; Enterprise Information Security Policy - Appendix A - CM-2, CM-5, CM-7, SI-2, SA-5) –Security practices dictate that new workstations and servers be imaged or configured from a fresh installation of the system's operating system. Traditionally, workstations and servers are configured by the manufacturer focusing on ease-of-use, and not security. By rebuilding or reimaging all workstations, this will provide for the distribution of a common system image for an agency to build upon. Due to the frequency that security updates are distributed from various software manufacturers, it is recommended that the "Gold Image" for workstations be updated on a monthly basis as well. System hardening should include the removing of any unnecessary system accounts or processes, closing network ports, and the use of additional security controls such as antivirus, intrusion prevention systems, and a host-based firewall. This "Gold Image" could be validated against security benchmarks from trusted sources. Vulnerability Scan must be completed on "gold image" and vulnerabilities are reviewed for impact and risks mitigated before deployment.

b. Patch Management (Enterprise Information Security Policy - 1.7.6, 1.7.10, 1.7.12, 2.11.6, 2.14.6; Enterprise Information Security Policy - Appendix A - SI-2)– It is imperative that all agencies develop and institute an effective patch management process for both workstations in order to remediate discovered, published threats. Policy dictates that no under-patched system or unsupported operating system or application is to be allowed connectivity to SummitNet. Agencies will need to develop an auditing process in order to ensure compliance with state policy. As a guideline, all patches should be deployed to their respective technology after appropriate testing.

c. Remove Admin Privileges Where Necessary (Enterprise Information Security Policy - 2.6, 2.9.5.3, 2.10.9, 2.19; Enterprise Information Security Policy – Appendix A - AC-2, AC-6, CM-7) – Standard end-users should not have administrator privileges on their workstations. Though it is often convenient for support staff to allow for end-users to have elevated privileges, the security risks this introduces are increased exponentially. Many flavors of malware typically include elevation of privileges in order to fully take advantage of an exploit and spread to critical information systems.

d. Deploying of EMET (Enterprise Information Security Policy – 2.7.1, 2.7.2, 2.9.6, 2.15.6; Enterprise Information Security Policy – Appendix A - SI-3, SI-4, SI-7, SI-16) – The Microsoft Enhanced Mitigation Experience Toolkit, or EMET as it is commonly referred to, is a useful and free tool provided by Microsoft for use by system administrators to augment workstation security. EMET will require some investment in time from resources administrating it and testing it before its introduction into an agency's environment, as unique applications used may cause conflicts that could inhibit business processes instead of securing them.

e. Applocker (Enterprise Information Security Policy – 2.6, 2.19.3, 2.19.4, 2.19.5 ;Enterprise Information Security Policy – Appendix A - AC-2, AC-3, AC-6, CM-7, CM-11, PL-4, SI-2)– Windows Applocker is a new application control and whitelisting feature in Windows 7 and Windows Server 2008 R2 that allows you to specify which users or groups can run particular applications based on unique identities of files. This is intended to replace the Software Restriction Policies feature. If AppLocker is used, agencies can create rules to allow or deny applications from running. AppLocker provides administrators with the ability to specify which users can run specific applications. AppLocker allows administrators to control the following types of applications: executable files (.exe and .com), scripts (.js, .ps1, .vbs, .cmd, and .bat), Windows Installer files (.msi and .msp), and DLL files (.dll and .ocx). This helps reduce cost of managing computing resources by decreasing the number of help desk calls from users running inappropriate applications.

With research, SITSD commonly sees malware run out of the following folders:

- **%OSDRIVE%\Windows\System32**
- **%OSDRIVE%\ProgramData**
- **%OSDRIVE%\Program Files**
- **%OSDRIVE%\Users\<*user*>\AppData\Local\Microsoft\Windows\Temporary Internet Files**
- **%OSDRIVE%\Users\<*user*>\AppData\Local\Temp**
- **%OSDRIVE%\Users\<*user*>\Downloads**
- **%OSDRIVE%\Users\<*user*>\Documents**

SITSD has also seen ransomware most commonly running out of the following folders (in order of frequency):

- **%AppData% – User > AppData > Roaming**
- **%Temp% – AppData > Local > Temp**
- **%UserProfile% – Current User Profile**
- **%AllUsersProfile% – Computer > C: > ProgramData**

Applications could be installed into a user profile without that user having administrative rights on the system. This is how advanced malware bypasses a system locked down without administrative rights. The ability to whitelist applications is another feature of Applocker that should be utilized. A combination of preventing executables from running out of common malware folders along with the whitelisting of applications with trusted digital signatures would be a significant improvement in hardening an OS with Applocker to prevent an infection.

f. Elimination of Mapped Drives (Enterprise Information Security Policy – 2.7; Enterprise Information Security Policy – Appendix A - SI-3) – This part of the Device Hardening Strategy may not be possible for agencies to adopt. The group has decided to make this a recommendation for agencies to consider if their business processes will allow for it. Malware, specifically ransomware if loaded onto a workstation, may target not only the device’s local drive, but also mapped network or attached drives as well. Ransomware looks for any other drives on the system, including mapped drives, and begins encrypting those files on the mapped drive as well. In an enterprise this could be catastrophic. By using shortcuts that point to a drive path you eliminate the ability for ransomware to find that drive and encrypt its contents. Simply putting the shortcuts into a folder and adding that folder into your favorites group on Windows Explorer makes the transition from using mapped drives to UNC shortcuts much easier for the end user.

g. Device drive encryption (Enterprise Information Security Policy – 2.1.9, 2.18.8, 2.9.2, 2.9.5.8; Enterprise Information Security Policy – Appendix A - IA-7, MP-4, MP-5) – BitLocker is a full disk encryption feature included with select editions of Windows. It is designed to protect data (in the event of physical loss of the device) by providing encryption for entire volumes. BitLocker is available in Ultimate and Enterprise versions of Vista and 7, as well as Pro and Enterprise versions of Windows 8 and 10.
BitLocker Drive Encryption can be configured to back up recovery information for BitLocker-protected drives and the Trusted Platform Module (TPM) to Active Directory Domain Services (AD DS). Backing up recovery passwords for a BitLocker-protected drive allows administrators to recover the drive if it is locked. This ensures that encrypted data belonging to the enterprise can always be accessed by authorized users.
Alternatively, BitLocker recovery information can be managed manually and stored securely using any of several widely available tools.

h. SmartScreen Filter (Enterprise Information Security Policy - 2.7.1, 2.7.2, 2.9.6, 2.15.6; Enterprise Information Security Policy - Appendix A - SI-3, SI-4, SI-7, SI-16) - SmartScreen Filter is a feature in Internet Explorer that helps detect phishing websites. SmartScreen Filter can also help protect you from downloading or installing malware (malicious software).
SmartScreen Filter helps to protect you in three ways:
    1) As you browse the web, it analyses webpages and determines if they have any characteristics that might be suspicious. If it finds suspicious webpages, SmartScreen will display a message giving you an opportunity to provide feedback and advising you to proceed with caution.
    2) SmartScreen Filter checks the sites you visit against a dynamic list of reported phishing sites and malicious software sites. If it finds a match, SmartScreen Filter will show you a warning notifying you that the site has been blocked for your safety.
    3) SmartScreen Filter checks files that you download from the web against a list of reported malicious software sites and programs known to be unsafe. If it finds a match, SmartScreen Filter will warn you that the download has been blocked for your safety. SmartScreen Filter also checks the files that you download against a list of files that are well known and downloaded by

many Internet Explorer users. If the file that you're downloading isn't on that list, SmartScreen Filter will warn you.

e. Windows Firewall (Enterprise Information Security Policy – 2.7.1, 2.7.2; Enterprise Information Security Policy – Appendix A - SI-3) - A firewall is software or hardware that helps prevent hackers and some types of malware from getting to your PC through a network or the Internet. It does this by checking the info that’s coming from the Internet or a network and then either blocking it or allowing it to pass through to your PC. A firewall isn't the same thing as an antivirus or antimalware app. Firewalls help protect against worms and hackers, antivirus apps help protect against viruses, and antimalware apps help protect against malware. You need all three. You only need one firewall app on your PC. Having more than one firewall app on your PC can cause conflicts and problems. We recommend that you use these default firewall settings:

- The firewall is on for all network connections.
- The firewall is blocking all inbound connections except those that you specifically allow.
- The firewall is on for all network types (Private, Public, or Domain).

5. Conclusion

This Device Hardening Strategy is the result of a multi-agency collaboration as well as has the MT-ISAC Best Practices approval. The representatives from these groups worked well together to endorse the recommendations contained here-in. A methodical, well-planned approach to effectively testing and measuring these controls will introduce additional layers to the security of the State of Montana’s end-users.