TEXAS AGRILIFE WORKSTATION HARDENING GUIDELINES

August 2012

The following describes a collection of both required and best practices methods related to the securing and hardening of security relative to workstations operated within Texas A&M AgriLife Agencies or the College of Agriculture and Life Sciences. All computer resource owners are expected to work collaboratively with IT resources to apply and maintain these guidelines.

Index

Workstation Hardening Guidelines Overview

The following guidelines have been developed in order to enhance security and quality operating status for workstations utilized within the Texas A&M AgriLife agencies and the College of Agriculture and Life Sciences. IT resources within the varied unit and centers are to utilize these guidelines when deploying all new workstation equipment. Workstation owners are expected to maintain these guidelines and to work collaboratively with IT resources to maintain the guidelines that have been deployed.

Questions regarding these guidelines or recommendations for improvement can be submitted to the Texas A&M AgriLife Information Security Officer.

Workstation Hardening Guidelines

1. Automated Patch Management

It is highly recommended that all patch management to workstations be automated and monitored through reporting with effective remediation procedures. To facilitate this model AgriLife IT has deployed a state-wide Windows Update Service for all workstations joined (or not) to the AGNET domain.

All workstations joined to the AGNET domain will automatically receive a policy update configuring the workstation to obtain its updates from an AGNET WSUS server. The unit will receive a report on a monthly basis showing any systems that have not successfully installed an update. Unit IT Resources should conduct a monthly remediation for any systems that are displayed on the report.

All county workstations in small county offices will obtain automated patch updates via desktop central. Desktop Central is managed by AgriLife IT and is dedicated towards the policy, patch, and security management for all county workstations. All county workstations shall have desktop central installed by AgriLife IT to facilitate this operational model.

2. Anti-Virus, Malware, Data Leakage Protection

All systems within the AgriLife Agencies and the College of Agriculture and Life Sciences are required to utilize Sophos for anti-virus, malware, and data leakage protection.

Distributions of Sophos are available through AgriLife IT Sophos Site (http://aitsophos.tamu.edu). Unit IT managers will have access to the Enterprise console to obtain alerts and perform certain remediation tasks.

3. Utilize Domain (centralized) Management Model

It is recommended that all units utilize the AGNET domain so that all general policies, controls and monitoring features are enabled for each workstation. In general, no system should be managed manually but rather through some central tool or model (i.e. Active Directory) in order to efficiently manage and maintain system security policies and controls.

4. Ensure non-required Applications are Removed

As with servers, it is recommended that any unused applications are removed from the systems. This may include any “bloat ware” provided by the OEM or manufacturer as well as certain applications like Java and peer to peer clients.

Note: Peer to Peer applications are prohibited by default per Agency rules and procedures for workstations operated by Agency personnel. An approved exception is required to operate such software as per the instructions in the rules and procedures.

5. Ensure all Applications are Updated at a Regular Interval (Automatic Preferred)

While the Windows update service will manage all Operating system update third-party applications also need to be updated and maintained. Fortunately a lot of third party providers now offer an automated update option for their applications. It is recommended that your workstations have automatic updates enabled for all third-party applications where available.

For those applications not offering automatic updates each unit should perform a regular review of system software version status and update accordingly. It is recommended that a quarterly review be performed so that software with security updates are not exposed to vulnerabilities for longer than necessary.

The AgriLife Information Security Office also sends out weekly notices on critical security updates for all applications and operating systems. Unit IT resources should review these notices and appropriately escalate actions to guarantee the security of workstations within their units. They should also forward any notices from the ISO office to their unit employees if the situation warrants escalated awareness by every employee.

6. Ensure that Web Browsers are Updated

One major avenue of access to computer workstations is through their Internet browser. It is highly recommended that Internet browsers on workstations always remain up to date at all times. Most all browsers offer auto-update features (or in the case of Microsoft Internet Explorer are updated with the OS updates).

Please ensure all browsers are set to auto-update and review quarterly to verify they are being updated within each unit.

Note: Sophos adds a component to each workstation to project users from navigating to sites that have known malware infections. This function works for all web browsers and will notify the user when they have navigated to an infected site and block access to the site.

7. Local Security Setting Recommendations

By default all workstations joined to the AGNET domain will obtain these security setting policies. If a unit is operating a system off of the AGNET domain it is required by state, system, university and agency policies that the following be applied.

A. Disable guest accounts
B. Disable Administrator Account (create an alternate account with Administrative Access)
C. Complex password setting must be enabled
D. Set min password length 8 characters
E. Set max password age 180 days
F. Set min password age to 1 day
G. Set password history to 12
H. Account Lockout feature must be turned on (recommend setting of no more than 4 attempts)
J. Disable file sharing (should be disabled by default on Win7)