CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

CSUSB Baseline Configuration for Services, Desktops and Mobile Devices

CSUSB Information Technology Services

Last Revised: **4/14/2020**

Final

REVISION CONTROL

Document Title: CSUSB Baseline Configuration for Servers, Desktops and Mobile Devices

Author: Javier Torner

File Reference:

Date	By	Action	Pages
9/18/2015	J Torner, J Macdonell	Created Document	All
4/13/2016	J Torner, J Macdonell	Edited Document	All
4/14/2020	G Au, J Macdonell	Edited Document	Page 3

Review/Approval History

Date	By	Action	Pages
4/14/2020	IT Governance TOCS Subcommittee	Reviewed and Approved	Page 3

CSUSB Baseline Configuration for Servers, Desktops and Mobile Devices

This document lists the security configuration requirements as required in the CSU and CSUSB Information Security Policies and Standards so that they can be implemented by all campus units as part of their deployment of computer systems.

Adherence to these standards can be through the deployment of group policy in the campus Active Directory and SCCM or through similar software management tools.

1. Common Configuration (Servers, Workstations, Laptops, Mobile Devices):

1.1. Operating System

1. Follow a CIS Benchmark and/or SCAP checklist. Use system configuration management tools (such as group policy, puppet, etc.) to bring the evaluation score to 70 or above.
2. Deploy using cloning (virtual machines), imaging software (e.g. ghost), or automated configuration management (e.g. puppet).
3. Configured with the latest stable release of operating system. Prefer long-term support (LTS) releases.
4. Joined as member of an enterprise directory.
    a. Windows: csusb.edu Active Directory.
    b. OS X, Linux: csusb.edu Active Directory (Kerberos, samba/winbind).
    c. Mobile devices: mobile device manager (mdm.csusb.edu).
5. Harden the OS off-line as much as possible to minimize exposure. Specific configuration steps, are listed below.
    a. Disconnect from Network.
    b. Install from a Trusted Source, usually a CD/DVD.
        i. Apply Patches, off-line if possible.
        ii. Install Applications, off-line if possible.
    c. Disable or restrict features and services — the benchmark will help.
    d. Configure unattended periodic (Automatic) security updates.
6. Install CSUSB Certificates.

1.2. Software

1. Install Identity Finder (or similar) where supported.

2. Install eDiscovery/Incident Handling software (e.g. EnCase Enterprise agent) where supported.

2. Server Configuration

1. Set a complex and nondeterministic local root/administrator password
2. Configure servers to log to an enterprise syslog system.
3. Configure server to allow for credentialed vulnerability assessments.
4. Services requiring authentication must be directed to the campus SSO for users authentication services (e.g. CAS, Shibboleth, Kerberos).

3. Desktop Configuration

All campus desktops should be configured as follows:

1. Be a member of the proper Organizational Unit (OU) in an Active Directory
2. Allow only authenticated access with unique profiles and logon credentials for each user, preferably domain credentials.
3. User accounts are not to be added to Administrators group.
    a. Exceptions must be authorized by a manager.
    b. Exceptions for administrative rights are to be provided through a separate local (non-domain) account (e.g.`\Joe Coyote`).
4. Shared passwords and guest accounts are not allowed.
5. Use imaging software (e.g. Ghost) to create a general image with the default settings and profiles to deploy to new machines.
6. Set a complex and nondeterministic local root/administrator password 7. Be configured with a supported release of Windows. Other operating systems are not to be used except when authorized by a manager.
8. Be configured for unattended automatic security updates.
9. Install and register a Systems Center Configuration Manager (SCCM) agent (or similar agent) to enable additional software updates, upgrades, and inventory.
10. Install the campus approved anti-virus and configured to get updates and report to the campus central console.
11. Use boot-up (BIOS) passwords for all computer systems and set strong authentication for all user accounts, including any accounts with administrative rights.
12. Enable screen savers with authentication (Locking passwords)
13. Disable automatic execution of files on external devices (e.g. disable AutoRun/AutoPlay).
14. Log user login events.
15. Enable host-based firewall.
16. Disable unnecessary services.

4. High Risk Workstation Configuration

4.1. Network Protection

In order to protect the high-risk workstation from malware and/or data exfiltration, network access must be limited. Additional network protection can be achieved by one or more of the following methods, to be determined by risk assessment:

1. Network traffic limited to the minimum necessary to perform business functions by use of isolated network segment with traffic restricted to authorized inbound and outbound ports and destinations. (Please note that this may be used in combination with a virtual desktop environment for other work functions (web browsing, etc.) in order to address productivity.)
2. Intrusion detection and prevention technologies which address hostile sites, malware, etc.
3. Software defined networking, user based and/or application-defined routing or similar use of technology to control connectivity.

4.2. Protection against "zero day" malware

For high risk workstations with operating systems commonly vulnerable to malware:

1. implement restricted outbound network egress.
2. configure application whitelisting to protect against "zero-day" malware.

4.3. Host-based Firewall

In addition to network firewalls, in order to prevent unauthorized access from other “local” hosts within the same local area network, a Host-Based Firewall must be enabled and configured to restrict access to only authorized hosts.

4.4. Security Event Logging

The High-Risk Workstation must be configured to log security events as specified in the CSUSB Log Management Standard.

4.5. Local Data Management

1. Use disk encryption, preferably full-disk encryption, to protect locally stored data in case of device theft. Ideally, the encryption should be centrally managed to allow for escrow, recovery, and revocation of cryptographic secrets.
2. Use automated network backups that utilizes by data-in-transit and data-at-rest encryption on par with the disk encryption

4.6. Physical Controls

1. Position monitors and printers so that others cannot see or obtain confidential or sensitive data.
2. Keep workstation and portable equipment and storage devices such as CD, DVD, tapes, USB drives or other removable storage media in an appropriately access limited location.

5. References

CSUSB Safeguarding Confidential Information
http://iso.csusb.edu/policies/csusb-safeguarding-confidential-information-20131206.pdf

CSUSB Web Application Standard
http://iso.csusb.edu/docs/CSUSB%20Web%20Application%20Standard_5.pdf

CSUSB Access Control Standard
http://iso.csusb.edu/docs/CSUSB%20Access%20Control%20Standard%20042115.pdf

CSUSB Vulnerability Management Standard
http://iso.csusb.edu/docs/CSUSB%20Vulnerability%20Management%20Standard.pdf

CSUSB Vulnerability Management Guidelines
http://iso.csusb.edu/docs/CSUSB%20Vulnerability%20Management%20Guidlines.pdf

CSUSB Log Management Standard
http://iso.csusb.edu/docs/CSUSB%20Log%20Management%20Standard.pdf

The Security Content Automation Protocol (SCAP)
http://scap.nist.gov/
https://web.nvd.nist.gov/view/ncp/repository

Center for Internet Security -- Security Benchmarks
https://benchmarks.cisecurity.org/