MARSHALL UNIVERSITY INFORMATION TECHNOLOGY COUNCIL

Standard ITP-42

Standard for Baseline Security of Servers

1. General Information:

Marshall University server administrators must take reasonable security measures to secure their hosts as outlined by this baseline standard. Ensuring proper computer security is a continual process. It is the frame of mind that there are real threats and part of a server administrator's job includes keeping users, data and transactions safe from these threats.

1.1. Scope:

This standard applies to all computer system administrators managing a computer server providing any type of service to other users and connected to the Marshall University Network (MUNet). The following standards define common sense security practices expected of all computer server administrators.

1.2. Authority: MUBOG Information Security Policy IT-2 and Marshall University Information Technology Council

1.3. Passage Date: April 18, 2014

1.4. Effective Date: April 18, 2014

1.5. Revised Date: August 19, 2019

1.6. Related Policies, Procedures and Guidelines:

MUBOG IT-1 Information Technology Acceptable Use Policy, MUBOG IT-2 Information Security Policy, ITG-4 – Guidelines for Data Classification, ITP-19 Information Security Incident Response Procedure, ITP-42F Server Baseline Security Registration Form.

2. Ownership and Responsibilities

A server administrator, upon connecting their server to the Marshall University Network (MUNet) is responsible for the security of that device in accordance with the MUBOG Information Security Policy (IT-2) and applicable Information Technology Council (ITC) standard, procedures and guidelines.

> Responsibility: A server administrator and their Department, Division or College will be held accountable when a compromise occurs. It is also expected that the administrator will demonstrate reasonable precautions to ensure the security of their hosts.

3. Registration

All servers will be registered with the Marshall University Office of Information Technology (MUIT). Campus Colleges, Departments and Business Units must use the ITP-42F Server Security Standard Registration Form to report to the MUIT servers running in their department. This registration form will include names and phone numbers of people to call in emergency situations including contact information during semester breaks.

Note: When security related issues arise and this information is not available or inaccurate, there may be no choice other than to disconnect a server without notice. MUIT must be notified upon discovery of any system breach or suspected system breach. MUIT reserves the right to disconnect any server which poses a threat to the campus network. Any server not following the above procedures will be considered unsafe, and as such poses a threat to the campus network and other systems.

4. Baseline Security for Servers

4.1. Location:

Servers should only be located in physically secured areas only accessible by authorized personnel. There is no substitute for physical security.

4.2. Services Supported:

Administrators should only run only the essential services on a server that are necessary for it to complete its designed task. Every service running should be regarded as a mode of entry. The number of entry points should be limited to only those needed.

> Note: The chance that a computer will be compromised is increased with the number of services being run. Therefore, it is expected that every administrator knows exactly which services are running and why they are necessary.

4.3. Security Updates:

The latest system patches should be applied regularly.

4.4. Virus Protection:

Server administrators are expected to install supported anti-virus software (where available) and regularly scan their servers to ensure system health.

4.5. Log-on Limits: Administrators should limit log-on retries.

Note: Password guessing applications have a greater probability of cracking a password if given ample opportunity. For most situations, MU Office of Information Security recommends account lockout after three failed log-on attempts.

4.6. Account Reviews:

Accounts must be regularly reviewed for inactivity, and any dormant accounts disabled.
Note: Old accounts should be terminated regularly. When people leave the University, administrators should have a clear deadline for account termination. Dormant accounts make attractive targets to intruders, since no one will likely notice the activity.

4.7. Local Accounts:

Whenever possible, accounts should be located on and authenticated against the MU Net ID system (Active Directory-based infrastructure). Administrators should only use local accounts when absolutely necessary.

4.8. Privileged Accounts:

Special care should be taken with privileged accounts (including but not limited to "root" for Linux and "administrator" for Windows), commensurate with the privileges afforded the account. Passwords for privileged accounts should be given only to people with a need for privileged access. For Windows Servers, the "administrator" account should be renamed.

4.9. Password Protection:

All accounts must conform to the Marshall University Information Security Policy and applicable password standards.

4.10. Service Banners:

Wherever feasible, a log-on banner, stating that the system is for authorized use only, should be displayed for anyone attempting to connect to the system.
Note: If possible, log-on restrictions (by time of day, by system address, etc.) should be implemented. All operating system, version/release numbers, and vendor information provided in log-on/sign-on banners should be limited or disabled. Providing this information makes attacks easier by allowing intruders to pinpoint hosts with known security vulnerabilities.

4.11. Backups:

Server administrators should conduct regular backups to protect important data. Backup retention should be consistent with applicable data retention policies.

4.12. Server Logs:

Logs of user activity must be retained for a period of time.
Note: MU Office of Information Security recommends that server logs be kept for at least six months. Logs should include (where feasible) the time and date of activities, the user ID, commands (and command arguments) executed, ID of either the local terminal or remote computer initiating the connection, associated system job or process number, and error conditions (failed/rejected attempts, failures in consistency checks, etc.). Logs should be checked for signs of malicious activity on a regular basis. Knowledge that logs are kept, acts as a deterrent to abuse. Logs are also essential in investigating incidents after the fact.

4.13. Sensitive Information:

Servers which contain sensitive data are to be registered with the Marshall University Office of Information Security. Sensitive data includes but is not limited to social security numbers, credit card numbers, student educational records, electronic health records and other personally identifiable information (PII) which if improperly disclosed, would result in a breach privacy or identity theft.(ITG-4)
Note: Extra precaution must be taken with systems containing sensitive data. As a result, proof of compelling reasons that a system needs to contain private information may be requested by MU Office of Information Security.

4.14. Remote Administration:

Vendor or consultants who wish to gain access to a server from off campus should be assigned a MU Net ID and provided with VPN access. The system administrator is responsible for requesting the account and VPN access for the vendor or consultant. In addition, that vendor or consultant may be required to sign a non-disclosure agreement before gaining access to a server.
Note: Many servers require administration by outside vendors or consultants. In these cases, it is preferred that this outside access be obtained by using a VPN account. The account allows for secure remote access to the server. In the case on Windows servers, Remote Desktop Services should be used through the secure VPN connection to administer the server. UNIX, Linux or Mac servers should use secure shell (SSH).

5. Incident Response

5.1. Response Procedure:

A server administrator must read and understand the Marshall University Information Security Incident Response Procedure (ITP-19) located at the following URL:
http://www.marshall.edu/it/files/ITP-19-posted.pdf

5.2. Incident Confidentiality:

Information regarding security incidents will be kept confidential by all parties involved. Only authorized personnel may disclose such information.

6. Compliance

MU Office of Information Security reserves the right to scan systems for known vulnerabilities. When vulnerabilities are discovered, they will be reported to the designated system administrator who will be expected to quickly act to close all known security vulnerabilities for which there are reasonable methods to close such vulnerabilities. If the administrator is unable to do this in a timely fashion, the Office of Information Technology is authorized to disconnect any networked device which may negatively impact management, reliability or integrity of the campus network (IT-1).

References:

Standard modeled after http://www.baylor.edu/its/index.php?id=43844