i.t.solutions
uahuntsville

SECURITY RECOMMENDATIONS FOR WINDOWS SERVERS

AUDIENCE

This document is for UAHunstivlle Windows server administrators.

PHYSICAL ACCESS AND ENVIRONMENT

- Maintain the server in a secure room with only authorized access.
- Ensure proper climate and power controls.
- Use a locking screen saver if servers are left unattended.
- For external devices, extreme precautions should be taken.
- Appropriate destruction of hardware containing sensitive information is required.

SERVICES AND APPLICATIONS

- Disable any unnecessary services or applications.
- Know what services should be running and which actually are running.
- Do not enable Internet Information Services (IIS) unless it is necessary. If it is, limit services.
- Do not install unnecessary software (e.g. Adobe Reader) unless the applications are essential.
- Do not browse the Internet from the server.
- If Remote Desktop must be used, set it for high encryption. Restrict access to specific IP addresses.
- Keep Operating System and applications updated. Monitor security web sites for patch issues.

Note: Patches can be tested on less-critical systems before applying to more critical systems.

SECURITY

- Warning banners should be posted on computing systems and servers. These security banners should inform all users that the system or application being accessed is proprietary, that it should be accessed only by authorized users, and that system use is monitored for enforcement purposes.
- Install anti-virus software and keep anti-virus software updated. Also install McAfee ePolicy Orchestrator (ePO) for UAHuntsville servers.
- Enable firewall and filter traffic to enabled ports. For most sensitive systems, Internet Protocol Security (IPSec) should also be implemented.
- Subscribe to Microsoft Security Bulletins.
- Data transmissions over the network should be encrypted.
- Protect the Security Accounts Manager (SAM). You can password SAM in Windows 2008, but care must be taken to not lose the password.
- Use of Microsoft baseline security analyzer is recommended.

- Regular backups must be done.
- For sensitive data, policies should be reviewed for encryption.

ACCOUNTS AND ACCESS

- Keep administrator access tightly controlled.
- Apply an accounts policy which will control passwords, when users can login, privileges, etc.
- Each user should be granted access to only those hosts, services, and data for which that user has a legitimate need.
- Require complex passwords for all accounts.
- Disable file sharing, if possible.
- Change default passwords and disable default accounts if possible. The administrator account can be renamed (with extreme care).

LOGGING

- Enable logging. If the system processes restricted or confidential data, extra logging should be enabled to track user session activity, changes to system files, changes to privileges, startup and shutdown of system. Some activities and information should not be logged. These include passwords and informational application queries.
- Excessive access attempts should be logged or cause lockouts or alarms, as appropriate.