Windows Enterprise Security
OU Manager Security Drilldown

Steven L. Kunz – ITS

May 14, 2010

The following recommendations apply to management of departmental OUs and the secured workstations and servers that reside within them. These steps are in addition to all the standard security-related issues such as system physical security, system and application software updates (Microsoft and all third party), anti-virus software, etc.

Compartmentalize

1. Never use personal accounts (used for desktop login, reading mail, web browsing, etc.) for administrative tasks. Use your personal account (with low or no privilege) for personal use and multiple separate accounts for each class of privileged, powerful use (file servers, print servers, web servers, etc.).
    - At a minimum create an "administrative instance" of your personal account by creating a "!" account for your NetID-based account in Windows AD. Use that account (you only - a separate one for each OU admin!) for administrative tasks.
    - Each OU admin logs into (or uses "Run As"on) secured systems with their own administrative account as needed. Include only personal "administrative instances" for your OU admins in the "!<OU name> Admins" group. This provides both accountability and greater security.

2. Never use "anonymous head" administrative accounts (such as a "!<YourOU> admin" username) for administrative tasks. Such "anonymous head" accounts are typically shared by several people, making accountability and password changes difficult. Use individual "administrative instances" (see above).

3. Service accounts (and "Scheduled Task" accounts) MUST have long (30+ character) complex pass-phrases and NEVER be used for personal logins. Service Accounts should never be anyone's "administrative instance" account.

4. Assign privileges on a "need" basis, sparingly. If someone simply needs the ability to deploy desktop systems they can be granted that power without full OU-admin privileges. Windows delegation of control is very granular.

Firewalls and System Restrictions

1. Place secured systems on non-routable (10.*) subnets when possible. Remember that this protects you from the world outside the boundaries of ISU, but not from people or compromised systems from within ISU.

2. Use IPSec firewall rules on each secured system to only allow specific systems to connect to it (especially via RDP). Use the Local Security Policy -> IP Security Policies on Local Computer (or suitable group policy) to create an IP filter list to restrict port connections (port 3389 in the case of RDP) to only the few secure systems you want to allow RDP from.

3. Use Active Directory Users and Computers to alter your powerful user objects to only be able to logon to specific systems. This list is set on the "Account" tab with the "Log On To" button. The list of "Logon Workstations" is the "Computername" (NetBIOS name) of each allowed system.

Safe Practices

1. NEVER perform administrative tasks (with an "administrative instance") from a system you have not personally secured and known to be clean of viruses, trojans, root-kits, keyloggers, etc. Be aware of social engineering ("Could you just login here with your admin account and fix this for me?").

2. Only perform the specific administrative tasks necessary on a secured system. **No** email or web-browsing on secured systems. Leave that for your personal system and account.

3. Restrict a secured system to a specific function (don't put multiple services on a single secured system).

4. Use "pass-phrases" not "passwords". A pass-phrase should be over 16 characters (the longer the better), contain 4-5 (or more) words, at least three character sets, and have one misspelled word.

Trust, but Verify

1. Monitor membership in powerful groups (this determines if anyone has given power to others).

2. Monitor the location of powerful user objects (this determines who has the delegated power of these accounts).

3. Monitor the "Logon Workstations" for powerful user objects (to see if they are somehow now allowed to login to unsecured systems).

The best form of monitoring is via scheduled tasks running automated scripts. Such scripts can check all the above values and email (or send some other form of alert) when security policies are broken. Of course you will want the "watchdog" protected from the people being monitored and provide some form of "exception" or "change" approval and auditing.

Advanced Techniques

1. Thin clients. These clients can have a read-only operating system and a minimum attack surface for infection. When used for remote access to protected servers (assuming all other safe practices are followed) they can provide added security.

2. Virtualization. Virtualized systems hopefully provide protection from rootkits and viruses that infect the "slackspace" outside the operating system on a hard drive. They do not necessarily protect against long term OS infections unless they are constantly rebooted from their virtual images.

3. Multi-factor authentication. If your powerful account requires "something you have" (a hardware token) in addition to "something you know" (a password) you have a edge as long as your powerful account can never login to (or access resources on) any system that does not have the token client software installed (this is where the "Logon Workstations" comes into play again).