searchWin2000.com Manageability

Oct 09, 2002 *a newsletter from TechTarget*

Windows 2000 in the Enterprise: Technology strategies in action

Mark Minasi talks security, part one

by Christine Polewarczyk, Associate Editor

If you missed the recent MCP TechMentor Conference in San Diego, then you missed an opportunity to watch and listen to industry icon Mark Minasi, who was consistently entertaining and educational. The biggest threat to corporate security, says Minasi, is not external attackers -- "it's that face in the mirror that you have to worry about the most." Read on for a recap of some pearls of wisdom from one of TechMentor's most popular presenters.

Set strict password policies

There is a password policy built-in to Group Policy for Windows 2000 that is also available as an add-on in NT4. When this policy is enabled, it:

- Requires six or more characters
- Requires three of these: capitals, lowercase, numeric, punctuation
- Doesn't allow the user name to be part of the password

To configure, go to Computer Configuration/Windows Settings/Account Policy/Password Policy. Apply as a domain policy; this doesn't work in OUs. Also, in this instance, don't leave the policy in its default location -- move it *above* the default domain policy.

Prohibit use of the default administrator account

No one should be logging in using the generic "administrator" account; there is no way to establish accountability if you do, even if you have auditing enabled. The best approach is to give individual user accounts administrative privileges as necessary, but discourage or even prohibit use of the actual administrator account.

There are a few things you can do to enforce the policy. First, you can randomize the admin account password. The cusrmgr tool in the Windows 2000

Resource Kit will do this for you (cusrmgr -u Administrator -p /domain). Or, if you're using XP or .NET, you can use the net user command (net user administrator/random/domain).

Another strategy is to have two or more admins share the admin password. Think of your system as a high-security vault that requires you to turn multiple keys in order to open it. If you have two admins, you could have a 10-character admin password with the first admin knowing the first five characters and the second admin knowing the last five characters. They would then have to work in cooperation to access the administrator account.

Also, rename your default administrator account. Changing your default administrator account can prevent a good 90% of attacks. A default administrator account doesn't really offer any security -- it will only protect you from stupid hackers. For security's sake, change this account from its default setting.

Auditing and logs: Use them!

Yes, auditing and managing logs can be cumbersome. But unfortunately, they just can't be ignored. Turn on security auditing and start collecting those logs! Even if you don't have time to review your logs regularly, at least you have a fresh trail to follow if something goes wrong.

When turning on auditing, use Policies to avoid having to manually set each server. Go to Local Security Policy/Local Policies/Auditing Policies. Also, turn on your auditing functions in two places: first enable auditing in either local group policies or domain group policies. Then, go to Properties for each object and turn on the level of logging. When setting levels, failures are usually more interesting and successes will fill up your logs very quickly.

And remember, logs do you no good if you never look at them. If possible, check the logs daily or use resource kit tools to export and filter them.

Services: If you don't need them, disable them

If you're not using a particular service, then shut it off. Fewer services mean less code, which means fewer bugs. Less code also means fewer security holes. Turning off unnecessary services also frees up more RAM that your system can use for other activities. Some examples of services that you might not need are:

- File server "server"
- Web server
- SMTP service
- Fax
- Messenger
- NetMeeting Remote Desktop Sharing
- RRAS
- Still Image Service
- Index service
- XP Web Client

If you are using any of these services, then keep them activated. Otherwise, you're just wasting CPU and leaving your network more open to security vulnerabilities.

Use split-brain DNS

Active Directory stores a ton of information about your network in DNS. This information is not something that you want the world to see. To avoid this, you can use split-brain DNS. Split-brain DNS means putting a primary external "acme.com" DNS server and a secondary external DNS server outside the firewall. Inside the firewall, have a primary internal "acme.com" DNS server and a local DNS server that will act as a secondary zone for the internal acme.com primary internal DNS server. Queries should be resolved by the primary internal DNS server and then sent to the primary external DNS server through a slave relationship -- not forwarding -- to secure your DNS.

One caveat: don't ever introduce the two primary DNS servers to each other.

Continue on to part two

MORE ON THIS TOPIC:

>>Read our expert security tips: How to protect networks without security overkill

>>Check out this Q&A interview: Five ways to stop hackers

ABOUT THIS E-MAIL: