

Re: Basic question from a security newbie

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-09/1297.html

From: Gordon Smith (eMVP) (Gordon.Smith_at_avnet.com)

Date: 09/05/03

Date: Fri, 5 Sep 2003 08:38:45 -0700

Anyone?

Gordon Smith (eMVP) wrote:

- > *Don't let the "MVP" fool you here... My MVP role isn't related to*
- > *security. :-)*
- >
- > *I'm trying to lock down a computer for use in an internet cafe. I*
- > *assumed the rational way to approach this is to set the default*
- > *security level under software restriction policies to "disallow" and*
- > *then list the few apps (internet explorer, etc.) as apps that are*
- > *allowed to run. Am I on the right track?*
- >
- > *Here's where I am getting confused. I set enforcement to apply to*
- > *all users except administrators (sounds logical). I set the default*
- > *security level to disallow. I logged out (even rebooted for good*
- > *measure), but my limited user accounts are still able to run*
- > *everything. For grins, I went back to the admin account and listed*
- > *"sol.exe" using a hash rule as explicitly disallowed. My guest*
- > *account can't run sol.exe now, but I had assumed that having a*
- > *default rule of disallow would have achieved the same result. Having*
- > *the sol.exe show up as blocked tells me that the policies I'm*
- > *changing do actually mean something to the system, but the default*
- > *rule of disallow seems to be ignored.*
- >
- > *Do I need to do something to have the default security level of*
- > *"Disallow" stick or am I misunderstanding what it means?*

--

Gordon Smith (eMVP)
Gordon.Smith@nosspam.avnet.com