

Re: Shared permissions vs. security

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-05/0358.html>

From: Steven L Umbach (n9rou_at_nospam-comcast.net)

Date: 05/27/05

Date: Fri, 27 May 2005 13:35:50 -0500

Did you have to make the users power users or administrators only after you changed permissions?? If so your changes are counterproductive in that they caused the users to be members of privileged groups which is something you want to avoid. There is nothing wrong with a user having full control or write/modify permissions to a folder if that is what they need to do their job but a normal user would not need full control to everything like an administrators would. For the drive root folder I usually give administrators and system full control and users have read/list/execute.

Regular users will not be able to install most software and that will require that an administrator do such or the use of Group Policy to assign .msi applications to the user or computer via Group Policy. If you as an administrator are having trouble installing an application or saving temporary files then permissions are too restrictive to the related folders. By default administrators and system have full control to all folders on the computer. There are free tools such as filemon from SysInternals that can help you track down when permissions are too restrictive. You could start filemon right before you try to update the antivirus for instance and then stop filemon from logging when the update fails and look in the filemon log for "access denied" entries which will show what file/folder you need to tweak permissions on.

<http://www.sysinternals.com/ntw2k/source/filemon.shtml>

In general when tweaking permissions start out with what you think should work and if that fails allow greater permissions until everything works. Windows Office applications can be a challenge in that they use temporary files that the user needs write and modify permissions for so you will need to give users greater permissions to those folders. Keep in mind that you can use creator owner [usually shown and with full control by default] in folder permissions so that the person who creates the file and becomes owner will receive permissions that the creator owner shows.

To answer the question for your original concern about worms and hackers in more detail be sure to follow these basic steps as a minimum.

— Require all users to use a complex password and that they are periodically changed and enforce via password policy. Make sure that users

do not share passwords. If users are not currently using strong passwords make sure they are forced to do such because you can implement a new password policy but until a user changes their password it will not be in effect. No or weak passwords are by far the largest vulnerability you can have on your network

— Verify that membership in the administrators group on all computers is what you expect and kept to a minimum.

— Use a properly configured firewall to protect your network and periodically check it by doing a self scan at a sites such as <http://scan.sygatetech.com/> .

— Make sure that your computers are kept current with critical security updates at Windows Updates. Your computers can be configured to do such automatically. Use MBSA to scan your computers periodically to make sure such is happening.

— All computers must be running a quality antivirus program. That program must scan ALL email attachments, be kept current with virus definitions which can be done automatically, and run in "autoprotect" mode. At least weekly full scans must be scheduled on each computer.

— Disable unneeded services on all computers including file and print sharing on workstations that do not need to offer shares/printers or be managed remotely via Computer Management. MBSA can help check for unneeded services.

— Never logon to a domain workstation that is not a known secured admin workstation as a domain administrator. Use a local administrator account instead.

— If at all possible make sure workstation users are regular users and not administrators or power user.

Though having proper share permissions is important all the above is much more important than share permissions to controlling worms and hackers. ———
Steve

"Carl Gross" <CarlGross@discussions.microsoft.com> wrote in message news:8EB83F35-F6D8-4E28-A830-EFF305720C66@microsoft.com...

>I have had to make some changes to some of the shares and groups because
>they

> were too insecure. Since then, I have had to add each user manually to
> each

> workstation with Power User privileges in order to do anything.

>

> I have also been changing the Security settings on each persons hard drive
> (default is Everyone – Full Control) and in some cases I need to make them
> Administrators to make install/uninstall easier. This works on most
> people,

microsoft.public.win2000.security: Re: Shared permissions vs. security

> *but some are perplexing me by not allowing me to install some software*
> *(antivirus updates in particular) and saving of temporary files for*
> *network*
> *applications.*
>
> *"Steven L Umbach" wrote:*
>
>> *I can't recommend settings but use the principle of least privilege. If a*
>> *user does not need to write to a share then give them only*
>> *read.list/execute*
>> *permissions.*
>>
>> *As far as hackers and worms make sure that users are forced to use strong*
>> *passwords via security policy, that the users are not local*
>> *administrators*
>> *if they do not need be, that you keep all your computers current with*
>> *critical security updates from Windows updates, that all computers have*
>> *antivirus installed that can keep itself current with updates*
>> *automatically*
>> *and that the antivirus runs in autoprotect mode and scans ALL email*
>> *attachments, and you have a firewall that protects your network.*
>> *Microsoft*
>> *makes a free tool called Microsoft Baseline Security Analyzer that can*
>> *scan*
>> *all your computers looking for basic vulnerabilities as shown at the link*
>> *below.*
>>
>> *<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>*
>>
>> *Microsoft also offers a free guide call Antivirus in Depth that is*
>> *excellent*
>> *in education users on what malware is, how it propagates, how to detect*
>> *it,*
>> *how to eliminate it, and how to prevent it. See the link below if*
>> *interested. The last link is a online guide from Microsoft for securing*
>> *small businesses. --- Steve*
>>
>> *http://www.microsoft.com/technet/security/topics/serversecurity/avdind_0.mspx*
>> *--- Anti Virus in Depth.*
>> *<http://www.microsoft.com/smallbusiness/gtm/securityguidance/hub.mspx>*
>>
>>
>> *"Carl Gross" <CarlGross@discussions.microsoft.com> wrote in message*
>> *news:18033C22-B195-4B50-91B8-208938BB23EE@microsoft.com...*
>> > *Can you recommend a security setting that I can enter to keep viruses*
>> > *like*
>> > *Backdoor.Trojan from propogating through (allowing people to work on*
>> > *the*
>> > *network and yet not allow THINGS or hackers permission to run amock).*
>> >
>> > *"Carl Gross" wrote:*

>> >

>> >> *I have been trying to make our network more secure by setting each workstation harddrive shared between Domain Admins with Full Control rights.*

>> >>

>> >> *What is the difference between setting this permission and selecting the Security tab to have the same permissions except adding the SYSTEM and user at that workstation?*

>> >>

>> >> *We have W2K SP4 workstations on a SBS 2003 server.*

>>

>>

>>