

Re: Least User Priviledges for Network Administrators

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2007-10/msg00318.html

- *From:* "Thomas M." <NoEmailReplies@xxxxxxxxxxx>
 - *Date:* Wed, 24 Oct 2007 11:54:16 -0600
-

Thanks for the response.

We've already covered most of the other security issues that you mentioned. We use Citrix in place of TS. By providing a Citrix desktop loaded with the appropriate tools and drive mappings, we completely negate the need for people to TS to their local PCs. If a person has data stored on the local PC then that person is in violation of an enterprise policy and is SOL as far as accessing those files is concerned (we require data to be stored on a network share so that it can be backed up, and so that it will be available via a drive mapping in Citrix). Administrative shares are strictly prohibited by our enterprise policies. Finally, the accounts that we use to administer local PCs have rights only on the PC—those accounts have no rights at the domain level.

--Tom

"Anteus" <Anteus@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:1E94CA45-887B-46A6-8E52-827FB00CE830@xxxxxxxxxxxxxxxxxxxx

"Steven L Umbach" wrote:

While implementing the principle of least privilege is a noble goal I think you might be over doing it with that group of users. Most likely they are all highly trained competent people very knowledgeable about computers and people you already trust as they have access to very sensitive areas of your network.

Agree, and the imposition of restrictions on sysops will be so frustrating that they will likely cease to do their jobs properly – which will further impact on security.

Re: Least User Priviledges for Network Administrators

I think if you want to improve security in the Administrative area, you could take a long hard look at the more vulnerable aspects of Windows' remote-admin schemes, for example the Remote Registry service, Terminal Services, and Administrative Shares (C\$, etc.) If you don't need or use these you can give a significant boost to security by turning them off. If you later find you DO need them, it's easy enough to turn them back on.

The other key point of course is that granting Domain Admin rights is a very different thing from granting local Administrator rights. Routine maintenance or helpdesk work should never be done under a Domain Admin account, as this exposes the entire network to any malware which might happen to be running on the faulty computer. Therefore, never use a Domain Admin logon anywhere other than at a known 'clean' computer, such as a server.