

Re: remote desktop issues

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-09/msg00107.html>

- *From:* "Jon" <jon.emmett@gmail.com>
 - *Date:* Thu, 27 Sep 2007 19:09:17 -0700
-

Al Dunbar wrote:

"Anthony" <anthony.spam@xxxxxxxxxxxxxxxx> wrote in message
[news:eIZNi3n\\$HHA.5328@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:eIZNi3n$HHA.5328@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Al.

Could it be that your IT security have got hold of the wrong end of the stick?

Perhaps...

– Remote Assistance: question is whether to require offer or not

We use SMS remote control for virtually any situation where Remote Assistance might serve as well. I believe that Remote Assistance is currently disabled by group policy (although it is checked as enabled on the workstations). Would enabling RDP also enable R.A, thereby requiring another configuration change to turn it off? That might be one almost valid reason for us to leave RDP off if it were the case, or at least it would require a stronger case for RDP.

– Remote Desktop: question is whether to log off a user's session or not

That could certainly be an issue. As would having a user logon and disconnect a remote administrator's session... I expect some protocol would need to be put established to deal with this.

– TS Shadowing: question is with user consent or not
I can see a privacy issue only with Shadowing without consent.

Re: remote desktop issues

I hadn't heard of TS shadowing before (although I knew that TS sessions can be remote controlled somehow), but after a quick look I agree. I'll have to look more closely.

If my request to allow RDP to XP workstations were granted, it would be only for accounts already noted as workstation administrators, so it would not be the privacy of the general user, but the privacy of what we might be doing on those workstations. I wouldn't mind some higher power in our organization being able to see what it is I am doing, but there will most certainly be cases where what is displayed is of a sensitive nature.

That said, since it appears that TS shadowing is done on a TS session on a server (that is doing an RDP to an XP system), and since servers are generally considered more sensitive than workstations, it might be more important to consider the privacy of TS sessions on the server before worrying about XP workstations.

I'll definitely need to think a bit more about this one...

You might like to break out the exact operation being performed through each method and ask which is the problem, e.g

Excellent suggestion! When I have discussed this informally, they seem tend to not want to get into specifics where their concerns could be examined in the light of day ;-)

- access to user's session
- control of user's mouse and keyboard
- access to files
- remote execution
- view user's actions (with consent)
- view user's actions without consent
- force user logoff or machine shutdown
- etc.

Anthony,
<http://www.airdesk.co.uk>

Thanks. You've given me a good start.

/AI

Re: remote desktop issues

"Al Dunbar" <AlanDrub@xxxxxxxxxxxxxxxxxxxxxx> wrote in message
[news:uqBoIdm\\$HHA.1208@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uqBoIdm$HHA.1208@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

I received the following private response from Steve B.:

Our company policy that each employee signs, contains a section stating that the computer and any data on it belong to the company and that IT management have the right to access that data if system maintenance requires it. Also, with RDP, having the user accept the remote control session could overcome one hurdle. As you say, files can be seen by IT without the need for RDP, however ignorance is bliss. If you are on a LAN that is protected by a firewall that blocks port 3389, then you would only be worried about internal access via RDP, in which case you can control remote access by allowing access to domain admins or similar groups only.

1) we have similar policies, however, my purpose in wanting to use RDP has nothing to do with looking at user files. IT security is concerned that if we have RDP access we could easily do so. As you say, though, if that is all I wanted to do I wouldn't bother with RDP.

2) my point about requiring the user to accept an RDP session is that I would rather avoid the user inconvenience by working on the system when they are not there. And, even if they were there, they could only say that it was OK for me to do so as far as they, individually, were concerned. But since I would be creating a second session and not connecting to theirs, who would give me permission to connect on behalf of the dozens of users not currently on shift who may have files on that system?
A completely illogical requirement in my mind, as I could swap

Re: remote desktop issues

the machine out with little notice and no permission if I felt I needed to examine it more closely in the shop.

3) I have no doubt that our firewall blocks port 3389. By default, members of the local administrators group would be the only ones with RDP access, and that group is already well controlled, consisting, as it does, of those who need local admin access to support the workstations.

I appreciate the information, but what I am looking for is some confirmation that using RDP in a relatively closed environment does not introduce unreasonable risk, and what risk factors, if any, are present. Oh, and did I mention that RDP access is already enabled on all of our servers? I use it to access our local resource server on which I am an administrator, but not the domain controller where I am not. RDP is provided for and used by the small number of centrally located domain admins for whom this would otherwise require an airline ticket.

/Al

"Al Dunbar" <AlanDrub@xxxxxxxxxxxxxxxxxxxxxx> wrote in message

[news:O8qstXh\\$HHA.3900@xxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:O8qstXh$HHA.3900@xxxxxxxxxxxxxxxxxxxxxxxxxx)

I have been having some difficulty in getting a request to modify our group policy to enable RDP on our XPSP2 workstations past IT security. In researching potential issues, the only ones I have found are some DoS vulnerabilities for which patches have been available for some time. In any case, our internal network is heavily firewalled against access from the outside.

We are already using SMS remote control, but it is configured to require the remote user's acceptance of our request to remote control their workstation, so not of much use when

Re: remote desktop issues

nobody is there. Also, if we log the user out and logon to an account with administrator access, the user could potentially close the remote control session and remain logged on with privileges.

I would see RDP as a useful addition to our arsenal of tools, with SMS remote control for user support, and RDP for workstation support.

I believe that one of the concerns we are seeming to work against is privacy of the user's session, including any files they may have created locally, such as on the desktop. Of course, we can already browse remotely to the local hard drive, seemingly with even less accountability than if we were to logon remotely. And we have the authority to take a workstation out of service and examine it directly – without having to inform the dozens of users that have profiles there.

Basically, I am looking for comments, either for or against.

Does anyone out there have information (or better yet, actual experience) to indicate that the benefits of using RDP for workstation management are either outweighed, or not outweighed, by any other factors that we have perhaps not considered? If there are security, privacy, or other issues,

I know this is a Microsoft Post, but another possible solution would be a third party product such as Script Logic. No I'm not here pushing third party, but I'm not aware of any Microsoft product that would do the same thing. Script Logic would give the user the ability to see what you're doing so there is nothing hidden it even works over a VPN connection, i.e. the user or yourself connected through a VPN connection. I have used it in a large organization and it was a life

Re: remote desktop issues

saver. Not mention the remote capabilities, you can manipulate GPO, and it gives a pretty good run down of system stats before you log in.

Worth a look.

.