

Re: Keep admins off of client machines

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-12/msg05051.html>

- *From:* "John Vollman" <nospam@xxxxxxxxxxx>
 - *Date:* Fri, 30 Dec 2005 11:55:24 -0600
-

SG,

Come on, spill the beans on this security 'problem'. I want to have a look.

JV

"SuperGumby [SBS MVP]" <not@xxxxxxxxxxx> wrote in message
news:uOAUPODGHA.4080@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

> the sharepoint admin is simple, just create a standard user account for
> them and elevate their priveleges in sharepoint.

>

> I can't comment on your '2 others' accounts, depends what activity you
> wish these people to perform.

>

> and then we get to the guts. The 'Domain Administrator' account is
> implicitly, and in some cases explicitly, defined as 'GOD' (note: the
> capitals are deliberate) for an Active Directory, messing with his
> permissions can lead to problems. The process of excluding your
> administration person from the domain admin account is complex and fraught
> with danger. FOR ONE, it is common for the alternative account you give
> such personnel to have the ability to change user passwords, for them to
> be able to change a normal user's password they also get the ability to
> change the Domain Administrator password. They must be `_trusted_` not to
> abuse this privelege. and here we get to the meat of my argument.

>

> I'm a consultant. I perform administration duties for a number of clients.
> I have at times been questioned about what access I may have to
> 'sensitive' information. My simple answer is 'I can steal it and sell it
> to your competitors, or, in a fit of rage I can delete the lot and send
> you broke'. By request many of my cliets have recently brought their
> `_complete_` offsite backup sets onsite for the day of my visit, I know it
> was complete because I control the backups. I could have happily sat there
> and blanked every tape, then formatted C: (actually, I have a CD which
> does a lot nastier thing, repeated pseudorandom writes to the HDD. It is
> designed to make data unrecoverable from such media. I could sit around
> saying 'sorry, server crashed' for the 20minutes or so it would take to

Re: Keep admins off of client machines

> make most disk sets unreadable). BUT THIS DOESN'T HAPPEN.
>
> Your Administrator must both be responsible and trusted. It is possible to
> 'delegate' some permissions to a lesser priveleged user but unfortunately
> it takes a thorough understanding of such priveleges to do so. The
> 'Administrator' is the only person who could implement such, and unless
> you wish to some day need to recover from an extremely complex scenario
> there's not much you can do (as a non-administrative owner) to help. This
> is not a 'windows' thing, all computer systems have this 'weakness'.
>
> A friend of mine recently called. He noticed what he considers a serious
> problem with security in relation to SBS User Templates and Exchange
> priveleges. I agree with him, the problem as described is, IMHO, a
> problem. Why do I mention this without going into detail? Because he is
> more familiar with AD than I, yet it has taken him from the release of
> SBS2003 to just a few days ago to notice this problem. What hope for the
> DIY administrator? none.
>
>
> "Nick" <nickmirro@xxxxxxxxxxxxxxxx> wrote in message
> news:urp8i3PDGHA.812@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>> We have an SBS admin, a Sharepoint admin and 2 others who go between our
>> SBS and local Linux server. Those helping administer the servers should
>> not have access to client machines as they contain patient records,
>> proprietary applications, etc. How can we prevent transient
>> adminstrators with admin status from logging onto client machines (unless
>> essential) since those machines contain sensitive data?
>>
>
>

• **References:**

- ◆ **Keep admins off of client machines**
 ◇ From: Nick
- ◆ **Re: Keep admins off of client machines**
 ◇ From: SuperGumby [SBS MVP]

- Prev by Date: **Re: Windows Update 2003 SP 1 KB909988 (relating to SharePoint Services)**
- Next by Date: **Re: Roaming Profiles**
- Previous by thread: **Re: Keep admins off of client machines**
- Next by thread: **Re: Keep admins off of client machines**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**