

Re: Internet Kiosk Group Policy

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2006-03/msg00387.html

- *From:* "D.P. Roberts" <DProberts@xxxxxxxxxx>
 - *Date:* Thu, 30 Mar 2006 08:40:10 -0700
-

"Mark Heitbrink [MVP]" <spam-only@xxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:%23L%23Gk68UGHA.5660@xxxxxxxxxxxxxxxxxxxxxxxxxx

Hi,

D.P. Roberts schrieb:

*In System, enable "Run only allowed Windows applications" and set it to only run IE.

Thats no solution, [...]

Sorry but this IS a viable solution and we've been using it in production for over a year. If your policy is strong enough such that users cannot get to or rename files, this works just fine (see comments below). :-o

It's still not, because you have to grant the user at least "change" in their %temp%. Copy a *.exe to %temp%, rename it ...

Like I mentioned above, you can configure policy tight enough so they can't even GET to their temp directory – they can't get anywhere on any drives whatsoever.

Just as an example, hide and deny the local drives and then type in "C:\" in an Office 2000 dialog ... just wait what happens ;:-)

Not true, at least in Office 2003. [...]

Re: Internet Kiosk Group Policy

That's why I took O2K as an example. NoDrives and NoViewOnDrives are only taking effect on the explorer API.

I'm using myself this option, but I wanted to show the problem with it. It's an endless discussion about what's secure and what is not. Hiding drives in explorer is IMO not, it's only a small piece of the whole set. The problem with some settings is, that they are only an restriction on the explorer.exe or e.g. cmd.exe all other ways are still open.

The Run menu can also be removed via group policy. All I'm saying here is that with the proper combination of policy settings you can achieve a very tight and secure environment.

Some further examples:

- Deactivating connect/delete a Network connection is only a setting that's working with the explorer and it's only in the GUI
-> net use still works
- Deactivating CMD: command.com still works and so "net.exe" can be used it's 8.3 but "~" exists ;-)

If you've got users who can 'achieve' local admin rights you've got even bigger problems. When configured correctly in a properly-secured domain environment, users will not be able to 'get around' this.

Just a little Worst Case:

... boot from floppy/cd/usb, overwrite the local admin password, log in, "net localgroup administrators yourdomainuser /add", regedit/regedt32 open ntuser.dat from your user, delete all \policies hive, deactivate winlogon service ...

This can be avoided by disabling bootup from anything other than the local hard drive in the BIOS and setting a BIOS password. Sure, a user could open the box, pull the CMOS jumper and clear the BIOS password, but let's be reasonable here! There's no such thing as being 100% full-proof secure with zero chance for compromise. And unless you're users are a group of IT criminals or you work at the University of Hacking and Virus Writing or perhaps a top-secret government agency, there's no need to go overboard here.

Sure, I can create always a scenario, where I can become a local Admin, the question is only, how long does it take me.

My prior posting just was intend to be some kind of a "wakeup call".

Re: Internet Kiosk Group Policy

Policies are a good way to secure your network, but the disadvantage is:

- the restricted settings work only under specific conditions and only with a specific application
- it's a question of "How inventive are my users"

Like I said before: It's an endless discussion.

Mark

--

Mark Heitbrink – MVP Windows Server

Homepage: www.gruppenrichtlinien.de

W2K FAQ : <http://w2k-faq.ebend.de>

PM: Vorname@Homepage, Versende-Adresse wird nicht abgerufen.