

Re: restrict software installation

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-05/0170.html>

From: Jens Benecke (mail-020527@jensbenecke.de)

Date: 05/27/02

Date: Mon, 27 May 2002 22:55:08 +0200

From: Jens Benecke <mail-020527@jensbenecke.de>

To: Gultarb0y@aol.com

On Fri, May 24, 2002 at 11:26:53AM -0400, Gultarb0y@aol.com wrote:

> *NT 4.0 SP6A STIG'd to NSA guidelines*
> *scenario:*

Hi,

no solution, just a few ideas what we do here, and perhaps you can do something similar.

> *The big guy wants me to let users surf the net responsibly (yeah*
> *right)) but restrict either their downloading OR AT LEAST the*
> *installation of software from the internet. I have less than 1..*
> *.. "1" so that for many installs, I have to undo that setting to load.*

I would do something like 'mount -o noexec /home', same for /tmp, as these are usually the only partitions my users have write access to. Preventing users from executing stuff on their home directory and in /tmp will effectively prevent them from running their own programs. Scripts are excluded of course (as long as the script interpreter lies somewhere else).

Is there some similar principle in Windows? Can you restrict people to their home directory only, at all? I seem to remember that e.g. MS Office wants write access all over the place, which makes life hard for a secure multi-user environment.

> *Looking for options, suggestions, places to look. Issue 1: Keep the*
> *installation of unauthorized software at a minimum in a 24x7 shop*
> *where 3 shifts share machines and outages could affect 3 users. I*
> *prefer installation to require admin access. User would then place a*
> *service request for the needed software.*

Another principle we employ here is 'rsync'. rsync is a free tool that synchronizes directories, files, or block devices (partitions) with an emphasis on 'minimize network transfers'. On booting, the user is given

SecurityFocus Microsoft: Re: restrict software installation

the option to boot normally or to restore a default system image from the network. As only the parts are transferred over the network (and written to disk) that have changed from the network image, this is really fast (usually under a minute for a 20GB harddisk).

I assume there is software that is able to do similar things for Windows, although a complete synchronization seems to be again made impossible by unique system and registry keys (the only exceptions we make are a few files in /etc which contain e.g. DHCP hostname, and log files).

- > *Issue 2) User's remove the password protected screensaver option*
- > *while logged in. Prior to fielding to users, these setting were*
- > *already configured in the registry for default users account and all*
- > *existing accounts on the machine. Users manually undo this. If I*
- > *remove the display option totally, users cannot customize the font*
- > *size to their own visual abilities.*

Perhaps you can control this via some scripting stuff? On our desktops, we can control almost every setting via DCOP (<http://www.google.com/search?q=dcop>) commands, which can be used from just about any scripting language there is (XML objects if everything else fails).

- > *option: a)Set NT group profile to remove the screensaver tab from user*
- > *display option? b)Other suggestions?*

Well, these were just some ideas. Perhaps they point you to the right direction. I have some Windows experience, but we don't do Windows here, so I can't give you concrete examples.

--

mfg, Jens Benecke /// www.hitchhikers.de, www.linuxfaq.de, www.linux.ms
This mail is an attachment? Read <http://www.jensbenecke.de/misc/outlook.html>

-
- application/pgp-signature attachment: stored

-
- **Previous message:** O'Malley, William: "RE: MS-SQL Blank Password Enumeration"
 - **In reply to:** Gu1tarb0y@aol.com: "restrict software installation"
 - **Next in thread:** Donald Voss: "Re: restrict software installation"
 - **Reply:**(deleted message) Donald Voss: "Re: restrict software installation"
 - **Reply:**(deleted message) Kurt Seifried: "Re: restrict software installation"
 - **Messages sorted by:** [date] [thread] [subject] [author] [attachment]