

Re: Software Audit & Enforcement – Required?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2007-10/msg00064.html>

- *From:* "Ben" <benb@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 9 Oct 2007 08:46:36 +0100
-

At the moment I report directly to the Operations Director, who is fairly IT savvy, so I've documented most of the network setup, and given him the domain admin password. Obviously this means I have to keep the documentation up to date any time I change anything, which can take a while. :-)

"GreenieLeBrun" <GreenieLeBrun@xxxxxxxxxxxx> wrote in message news:%23th2EPjCIHA.3848@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

I can't add any info, but, I do have a question for you regarding the risk management policies of your organisation. If you are the only Admin for your domain what happens if an elephant falls out of a jumbo jet and lands on your head or some thing else happens that renders you no longer functional? Who then has access to the Admin rights on the companies domain?

Ben wrote:

Hi,

Thanks for the reply.

The local admin account on each laptop is disabled by default, and we have a domain wide group policy that uses restricted groups, the only group added to the local administrators group is domain admins, and that group only contains my admin account, plus I'm the only IT /Support person on site, for the moment (1 admin 25 users) so in theory, no user should ever be able to get local admin access to their machine.

Point taken on the privilege escalation by buggy software though. And we'll probably be employing a junior IT support person as the company grows beyond 25, so I guess it'll be useful to make sure they're not giving users admin rights.

Do you have any recommendations on what software can best accomplish this?

Many thanks

Ben

Re: Software Audit & Enforcement – Required?

<jwgoerlich@xxxxxxxx> wrote in message
news:1191838537.655344.286650@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello Ben,

An argument for auditing installed software? The maxim "prevention is ideal, detection is a must" comes to mind.

You prevent people from installing software by removing them from Power Users and Administrators. Now, the only point in time that you can be certain that the users were not administrators is when you last checked.

What can happen? Some obliging admin or helpdesk may add the person back into these groups at a later date. Or perhaps the person learns the local Administrator password. I have seen both of these happen, as well as the less likely privilege escalation bug installing software. Running a regular audit against the machines is your detection control. It lets you catch any exception. As an added bonus, this may give you an early indication of colleagues who are passing out admin memberships or credentials.

Regards,

J Wolfgang Goerlich

On Oct 8, 5:11 am, "Ben" <b...@xxxxxxxxxxxxxxxxxxxx>
wrote:

Hi,

I'm looking for some advice on software auditing and enforcement, and I don't know whether I'm trying to talk myself into this, or our IT Director out of it!

Re: Software Audit & Enforcement – Required?

Here is the situation: Until a couple of months ago, all our users had local admin rights on their laptops – bad idea I know – 4 months ago I finally got management to support me in removing users admin rights, at which point we decided to take a software audit to make sure there was nothing unlicensed/against company policy installed. We did this using sysinternals psinfo, which exported the software list for each machine to a text file. I then imported all of the files into excel, removed duplicates, MS hotfixes & updates, leaving me with a list of just the installed applications, which was about 700 long. I then sorted through this list, categorising each app into 1 of 3 categories, 1= must have, i.e. Symantec Firewall, Acrobat Reader, MS Office etc, 2=Can have, i.e. Acrobat Pro, MS Visio etc, 3=Can't have, games, p2p apps, unlicensed software etc. We then publish this list on the internal intranet for our users, if they have any cat 3 software, they have to remove it (if it requires admin access they come and ask IT dept).

This audit is something that management want to run on a regular basic, but they know how long it took to collate and sort through so they want a piece of software that can audit each machine, compare the results against the list of categories, and remove anything that is banned, or push out anything

Re: Software Audit & Enforcement – Required?

that is required.

However, most of these laptops, probably 75%, are either over 3 years old, or coming up to 3 years, which is usually the time that we'll scrap them, and buy replacements. I think half of that 75% will be replaced this side of Christmas, with the other half being scheduled for replacement in February.

The rest have been replaced, with a standard build, recently, AFTER we removed admin rights from everyone.

So, I'm trying to think of a situation when we would actually need to run an audit, and enforce the software policy. If users have a standard build, with updates being pushed out via WSUS, and new packages installed via GP software installation, and can't install any software themselves, will we ever need to enforce the software policy?

Does anyone have a good argument for needing a package to enforce a software policy when users don't have local admin rights? If so, can you recommend a software package? Does System Center Configuration Manager 2007 have this functionality?

Many thanks

Ben