

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@xxxxxxxxxxxxx> 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@xx

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 th