

Security breach

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-02/1460.html>

From: bp (*anonymous_at_discussions.microsoft.com*)

Date: 02/18/04

Date: Wed, 18 Feb 2004 12:29:17 -0800

I would advise you to get a lawyer as well, but if your relationship is otherwise amiable with your employer and they are purely acting per their security policy, you can suggest that they have a forensic expert analyze the hard drive. There is usually an abundance of evidence available that can at least indicate user behavior if not probable identity. This data could be correlated with the times that the suspect accounts were created. You would probably never get to see this data unless you are on good terms with them. If you are innocent as you maintain, it should at least provide some explanation as to when, where, how, why, what was done. It is also critical that they power off that pc and lock it up if the goal is to perform forensics work. Good luck.

>-----Original Message-----

>

>I've been suspended from work because I was accused of creating some

>accounts without going through due procedure. I did not create the

>accounts. Even if someone knows my user admin password shouldn't they

>be able to tell from the security log:

>a) which machine they were logged into ('cos it can't have been mine,

>via the IP)

>b) what time and date it was done (and compare it to when I was on my

>machine)

>c) could someone have manipulated the security logs and is it

>traceable

>d) what other possibilities should I be investigating, as to how

>someone has used my machine/log in & does it help me if my company has

>key stroke logging?

>
>*I have to go in on Friday to discuss this & I'd really*
appreciate some

>*help*

>

>*Thanks*

>

>

>*Annita*

>-----

>Posted via <http://www.mcse.ms>

>-----

>View this thread: <http://www.mcse.ms/message402926.html>

>

>.

>