

Re: Possible inside security breach

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-08/1085.html>

From: Oli Restorick [MVP] (oli_at_mvps.org)

Date: 08/28/04

Date: Sat, 28 Aug 2004 10:46:17 +0100

Agreed.

In fact, if you have a user account, you wouldn't even need to have your machine joined to the domain to gain access to data. Connection to the network is all that's needed and a VPN connection gave him that.

So, as far as I can see, no "hacking" or "security breach" has taken place here.

Oli

"Paul Adare – MVP – Microsoft Virtual PC" <padare@newsguy.com> wrote in message news:MPG.1b9a189b779474f7989a41@msnews.microsoft.com...

> *In article <[1c8f01c48cde\\$b45f7680\\$a501280a@phx.gbl](mailto:1c8f01c48cde$b45f7680$a501280a@phx.gbl)>, in the*

> *microsoft.public.win2000.security news group, G. Lentz*

> *<anonymous@discussions.microsoft.com> says...*

>

>> *1) I need to clarify that only an account with*

>> *Administrative privileges can create new user and*

>> *computer accounts in an AD domain?*

>

> *User accounts yes, computer accounts, no. This, to be quite honest, is a*

> *pretty basic AD concept, and I'd certainly expect any consultant working*

> *for me (that was doing anything at all with AD) to know this. In AD,*

> *every domain user account can add 10 workstations to the domain. Since*

> *the person in question obviously already has a domain user account, it*

> *is really just a matter of connecting to the domain through the VPN, and*

> *then adding his computer to the domain.*

>

>>

>> *2) Any possible ideas on how the hell they could have*

>> *done this? Don't need specifics, just could/can it be*

>> *done? I understand by the user having VPN access to the*

>> *network he basically had a key so to speak, allowing them*

>> *to bypass the normal things that discourage external*

>> *attacks (i.e firewalls).*

>

> *See above. If this wasn't supposed to be allowed, it certainly wasn't*

microsoft.public.win2000.security: Re: Possible inside security breach

> *the contractor's fault. It was whomever setup the remote access and
> allowed this to happen.*
>
>>
>> *I am going to try and speak to the client principal that
>> if they circumvented network security, then his network
>> is basically open at this point. Unfortunately the
>> principal is high on this person and their abilities so I
>> may be creating an acrimonious situation by bringing it up.
>> My thinking is I don't want to be blamed for something
>> down the line as I feel I no longer have control over the
>> network. Thanks.*
>
> *Again, as above. Given what you've told of the story here, you _are_
> responsible for this situation already.*
>
> --
> *Paul Adare*
> *This posting is provided "AS IS" with no warranties, and confers no
> rights.*