

Re: Controlling server security -- to domain or not to domain?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-12/0771.html>

From: Charles Otstot (*saries_at_notmyreal.address.com*)

Date: 12/11/03

Date: Thu, 11 Dec 2003 11:18:53 -0500

"Daniel Billingsley" <dbillingsley@NO.durcon.SPAAMM.com> wrote in message news:ewMPauzvDHA.2448@TK2MSFTNGP09.phx.gbl...

> *Well, I disagree. We're not really talking about "standalone" servers in
> the pure sense, as they all have to be part of the network, accessed by
> users and applications who must supply credentials of course. So at the
> very least you have a bunch of servers physically on the network that each
> has its own SAM database. I would guess that someone who has compromised
> one of those boxes would find enough information on it to get the next
> server, and the next, and so the dominoes would fall. Assuming the DCs
are
> especially secured (including physically), adding these other servers to
the
> domain actually improves security in this regard in my mind.*
>
> *I guess maybe I'm taking somewhat more of a pragmatic view here. With
> several layers of firewall and (I presume) NAT, etc., as the OP described
he
> has in place, it seems to me the biggest risk to these servers is from
> within the organization. That is to say, I'd say the risk from internet
> attacks has been mitigated to a satisfactory comfort level already,
> regardless of whether they're added to the domain or not. Adding a server
> to the domain, changing the local administrator NAME, and giving it an
> uncrackable password seems like the obvious way to go to me.*
>
Daniel,

I don't disagree at all that, if properly secured otherwise, domain membership for at least some (otherwise considered standalone) servers may be acceptable and even desirable. And to the extent that internal users and/or devices connect to those servers **and** that those servers must be connected to the internal network, I would agree that securing those servers via the domain may be the best way to go.

Where I disagree is in the (apparent) viewpoint that this is **always** preferable. About the only absolute I've found in this industry is that

microsoft.public.security: Re: Controlling server security -- to domain or not to domain?

there are no absolutes. Let's assume that the OP has a single webserver with a single public site facing the Internet, with no internal access (other than perhaps browsing the site) required. Let's further assume that the content on the webserver is small in size and is fairly static, requiring updates only quarterly. Let's further assume that the OP has available a DMZ that is not connected (but can be) to the internal network. Finally, we can assume that this is the only server that may (or may not) go into the DMZ.

In this scenario, it would seem to me that the risks associated with connecting the DMZ to the internal network and making the server a domain member might very well outweigh the benefits of using domain security. Without connectivity, if the box is compromised, only that server can be compromised. Yes, some account information may be gained that may be useful in attacking domain accounts, provided the attacker can find another point to jump to the internal network; but assuming sufficiently strong passwords and using a different naming convention for domain accounts, this risk can be easily minimized. On the other hand, if the server is a domain member connected to the internal network, with ports now necessarily open that would not have been otherwise, it could easily become an attractive jumping off point to the remainder of the network.

Obviously the above is more the exception than the rule today, but it does illustrate the fact that every installation decision is independent and the major options must be weighed with an open mind and with respect to the instant scenario. I would rather ask the questions and verify what works for the given situation. Given the information that was initially provided by sP, it still seems to me that the *question* was valid and (given the initial information) a case could be made for what he/she was considering.

Hope this clarifies my statements a little better.

Charlie