

Re: OWA 2003 in DMZ ??

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2004-02/3512.html>

From: Al Mulnick (*amulnick_No_SPAM_at_ncDOTrr.com*)

Date: 02/21/04

Date: Sat, 21 Feb 2004 11:57:32 -0500

Right. Thought I answered that but let me reiterate: High security is not something you'll be able to accomplish in that scenario that you have setup. Ports are mostly the same as E2K in E2K3. The setup you described should only need tcp 80 to the BE server and then just about all ports to the other DC's, DNS, etc. I haven't checked, but IPSec tunnels may be an option for you. You could specify the IPSec tunnel and simplify your port configuration (two ports and a protocol to set up IPSec, but you have to allow that conversation from all DC's/GC's, Exchange BE servers that the FE server will talk with. Since it's a DC, that would be about all of the ones you have potentially.) Note that Microsoft's recommendation is not to deploy DC's for your internal domain in your DMZ. Also note that their recommendation is to publish with ISA and greatly reduce the risk associated with complexity and traffic. The thinking is that stateful inspection is a thing of the past. For security, you want to use layer-7 devices since stateful potato passers will accept on one side and throw it over the (fire) wall. There really is no insight into the intent of the data stream. That said, you'd really want to limit the traffic that comes in and goes out and what the user can do if using a stateful inspection firewall device. In your case, you've blurred the line between inside and outside because you've put the internal data (the DC) on the outside of the castle. Now an attacker wouldn't have to go inside your network to gather data, right. It would be expected traffic to the potato passer, so it would happily let it gather whatever information the attacker wanted (password required of course). What I'm suggesting is a rethink in the approach you are using. If that is not possible, I certainly understand and wish you the best of luck either way. Be sure to check out <http://www.microsoft.com/security> for information on hardening the servers from an OS, DC, and Exchange perspective. Lot's of good information there but note that you won't be able to secure it completely.

Dan, I know it's possible to setup a certificate and last I checked it was a supported configuration to have a cert on the BE server. Can you verify that's still the case or not? That was last checked in E2K.

Al

microsoft.public.exchange.admin: Re: OWA 2003 in DMZ ??

"goofy" <ole.madsen@noosspam.omc.dk> wrote in message
news:e\$EY8aJ%23DHA.3496@TK2MSFTNGP10.phx.gbl...

> *Hi Al*

>

> *My question was how to implement high security in my FE-BE configuration,
> and then i explained how i have installed my testlab.*

>

> *We dont have an application firewall, but "only" a statefull inspection
> (SonicWall 4060), but that should be enough :-)*

>

> *To Dan.*

>

> *Is exchange 2003 using/need the same ports as exchange 2000 ??*

>

> */Ole*

>

>

> *"Dan Townsend [MSFT]" <dtown@online.microsoft.com> skrev i en meddelelse
> news:O\$i6%235I%23DHA.2316@TK2MSFTNGP11.phx.gbl...*

>> *"443 only comes into play if you have installed a cert on the BE"*

>>

>> *The cert can only be on the Front-End in a F/E->B/E config.*

>>

>>

>>

>> *I think you really should visit these links and consult the setups that
> are*

>> *provided. Otherwise get rid of the front-end and just allow 443 to the
>> back-end and give it a cert.*

>>

>> *Outlook Web Access for Exchange 2003*

>> *<http://www.microsoft.com/exchange/owa/>*

>>

>> *Using Exchange 2000 Front-End Servers (Yeah I know it says 2000 but its
> the*

>> *same concepts)*

>> *<http://www.microsoft.com/downloads/release.asp?releaseid=43997>*

>>

>> *Securing with something like IISLockdown is good but make sure you
> properly*

>> *configure the ini so it doesn't break OWA.*

>>

>> *--*

>> *Hope that helps,*

>> *Dan Townsend*

>>

>> *This posting is provided "AS IS" with no warranties, and confers no
> rights.*

>> *Please do not send email to this address, post a reply to this
newsgroup.*

Re: OWA 2003 in DMZ ??

> >
> > *Use of included script samples are subject to the terms specified at*
> > <http://www.microsoft.com/info/cpyright.htm>
> >
> > "Al Mulnick" <amulnick_No_SPAM@ncDOTrr.com> wrote in message
> > news:uj3nYTI%23DHA.3828@TK2MSFTNGP10.phx.gbl...
> > > *Why bother? Since you're putting it on a DC, there's really no point*
in
> > > *trying to secure it now is there?*
> > > *Since you're not using a layer-7 firewall that understands the calls,*
> *why*
> > > *secure the transmission?*
> > >
> > > *I throw that out there, but I also realize that there's more to it*
than
> > > *that. Don't get me wrong, I think that we have to work in the*
confines
> > > *we're living in, but what you're doing seems more like an exercise in*
> > > *futility.*
> > >
> > > *The comm between a FE and BE server is tcp 80. 443 only comes into*
play
> > *if*
> > > *you have installed a cert on the BE. Other options would be to use*
VPN
> > > *tunnels. The FE server normally needs to talk with other domain*
> > *controllers*
> > > *etc, but you've short-circuited that by placing on a DC already. It's*
> > *smart*
> > > *enough (out of the box) to know that you don't need to go to other*
domain
> > > *controllers since there's one local that's "less expensive" to use.*
> > >
> > > *Putting all of that together, is there really any reason for you to*
have
> > *put*
> > > *this in the DMZ? I mean, you're network directory is in the DMZ, your*
> > > *application is in the DMZ, effectively moving your border out into the*
DMZ
> > > *(you've put what you're trying to protect on the outside of the castle*
walls
> > > *so to speak).*
> > >
> > > *Good luck.*
> > >
> > > *Al*
> > >
> > >
> > > "goofy" <ole.madsen@noosspam.omc.dk> wrote in message
> > > news:uFPYrDI%23DHA.4088@tk2msftngp13.phx.gbl...
> > > > *Hi All*

