

Re: Question about DMZ Domain Member and Virus Membership

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-03/msg00269.html>

- *From:* "Adam T" <123security@xxxxxxxxx>
 - *Date:* Wed, 22 Mar 2006 07:00:30 -0500
-

Thank you both for your comments.

Now to follow this up further. If I shut down un-needed services and restrict access to machine ports from the internet as needed IE port 80 on one machine, port 25 on another. what else is recommended? What is the next goal/level to try to achieve.

On 20/03/06, Dan Bogda <dan.bogda@xxxxxxxxxxxxx> wrote:

They should have as few connections into your network as you can afford. Ideally you are building a DMZ to insulate your internal network from external threats. If you are building the DMZ to shield your Domain from windows threats it doesn't make sense to extend that Domain into the DMZ. There are always exceptions based on acceptable risk, budget and business requirements. This really comes down to a question of the risks and benefits the various options present for your company/client and how willing they are to accept them.

For example, if you are adding a lot of users or duplicate users it may make sense to allow the DMZ hosts to participate in the domain rather than manually updating two sets of hosts. Or, same scenario, it may make more sense to hire a contractor to create an automated event that can push changes to your DMZ, instead of the DMZ hosts participating in the domain and pulling updates. You should really document your options, the risk and benefit of each and let management decide what is worth pursuing.

In short, best practice would be to leverage the DMZ and not allow it to connect into your internal network. Instead, configure this as a no man's land and only allow connections into the environment, not out. Harden your DMZ boxes, disable unused services and don't put anything on there you are worried about losing. If clients are uploading files, pull them off as soon as you can. The more valuable data sitting on a DMZ host the more valuable a target it becomes.

Of course, this is just another opinion and carries no guarantees. Your actual mileage may vary. Hope this helps, good luck.

-----Original Message-----

Re: Question about DMZ Domain Member and Virus Membership

From: Adam T [<mailto:123security@xxxxxxxx>]
Sent: Sunday, March 19, 2006 6:01 PM
To: security-basics@xxxxxxxxxxxxxxxxxxxxxx
Subject: Question about DMZ Domain Member and Virus Membership

I would like to know what is the best practice method to configure Windows Servers in the DMZ. Should they be a part of the domain and therefore open ports to allow authentication? Or should they be kept as standalone servers? I also have my virus scanners on these machines but they are not in contact with the Primary Virus Server should I allow these ports through the firewall? Currently they are standalone virus scanners. Please share with me your thoughts on these configurations.

Thank you

./Adam

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The Norwich University program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience.

Tailor your education to your own professional goals with degree customizations including Emergency Management, Business Continuity Planning, Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The Norwich University program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience.

Tailor your education to your own professional goals with degree customizations including Emergency Management, Business Continuity Planning, Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>
