

Re: Need Help with Anti-Relay

Source: <http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.setup/2004-02/0907.html>

From: JP (*NO_SPAM_PLEASE_pangjo_at_netzero.com*)

Date: 02/16/04

Date: Mon, 16 Feb 2004 10:02:02 -0500

Dan,

Thanks for the direction to the KB. Now I have a better understanding of the security on Exchange against relaying and address spoofing. I am a little bit disappointed, though, for being not able to find a simple and effective solution to protect my mail server against address spoofing. I do not want a email sent from any foreign parties to be showing as someone in our organization.

The two solutions I have tried has drawbacks of its own:

1. ResolveP2 – I can edit the registry and change the address resolution default. When a user receive a suspicious message with a sender's name being someone in our company, they can check the message header to see if there is any Internet header. There are two disadvantages: a) the message will still be able to be delivered to the user's mailbox, it has not been blocked; 2) users have to be "educated" to read the header.

2. Reverse DNS Lookup – I can enable Reverse DNS lookup in the SMTP virtual server (from the Advanced option in the Delivery Tab of the SMTP virtual server properties). Then I can block messages which has a different DNS record than what appears on the sender's identity. Again, there are also two disadvantages: a) it takes up more system resources and slows down the performance as every incoming mail will have to go through the same process; b) some senders may not have their email server DNS record set up exactly to match the email domain, that is likely the case when an ISP is using one server to provide mail services to multiple organizations.

My goal is very simple. I want to block all incoming mail which has a sender's domain showing as internal (e.g. valid_user@my_domain.com) but bear an Internet header. I suppose that all email messages originated internally are sent either from the internal network or through Outlook Web Access. In both cases, there should not be any Internet header attached.

I think this is just a very simple requirement but as a new Exchange administrator, I am not capable of doing it.

"Dan Kelley [MSFT]" <dankel@online.microsoft.com> wrote in message news:e07TO1Y8DHA.2656@TK2MSFTNGP11.phx.gbl...

microsoft.public.exchange.setup: Re: Need Help with Anti-Relay

> *Hello JP,*
>
> *That's why the ResolveP2 functionality exists. It prevents spoofing*
> *(that's*
> *what you're talking about here), but does add quite a performance hit*
> *depending how deep you go with it. For more information, please refer to*
> *this KB article:*
>
> *288635 XIMS: ResolveP2 Functionality in Exchange 2000 Server*
> *<http://support.microsoft.com/?id=288635>*
>
> *Here's the Exchange Server 2003 version of this article as well:*
>
> *828770 Resolve Anonymous Senders Functionality in Microsoft Exchange 2003*
> *<http://support.microsoft.com/?id=828770>*
> --
> *Regards,*
>