

Re: Security Issue with ISA and Exchange Front end

Source:

<http://www.tech-archive.net/Archive/BackOffice/microsoft.public.backoffice.smallbiz2000/2004-06/1221.html>

From: Mark Arnold [MVP] (mark_at_mvps.org)

Date: 06/21/04

Date: Mon, 21 Jun 2004 09:56:02 +0100

"Srinivas" <srini_q8@yahoo.com> wrote:

>Hi All,

>Any comments and feedback would be appreciated.

>

>Scenario 1:

>Exchange FE(Front End) in DMZ and BE(Back End) in the Internal Network and a

>Dedicated Firewall(not ISA) protecting our network.

>I provide OWA on http port 80, POP3 and SMTP access via internet. These are

>the only ports I open for the Internet users to the FE, and precisely the 6

>or 7 ports I open on the dedicated FW(Firewall) for the FE to talk to the BE

>

>Concern:

>If there is a buffer overflow vulnerability or for that matter any

>vulnerability and the attacker compromises the FE Server what kind of risk

>is involved with the backend server.

>

>

>Scenario 2:

>ISA in DMZ and not a member server of my Domain, FE and BE in the Internal

>Network and a Dedicated Firewall(not ISA) protecting our network.

>I provide OWA on http port 80, POP3 and SMTP access via internet. These are

>the only ports I open for the Internet users to the ISA, and precisely the

>ports 80, 25, 110, and 53 I shall open on the dedicated FW(Firewall) for the

>ISA to talk to the FE.

>

>Concern:

>If there is a buffer overflow vulnerability or any vulnerability on port

>80/110/25 the attacker straight away compromises the FE in the Internal

>Network rather than the FE in the DMZ like it is the case in Scenario1. If

>he succeeds then he may gain complete access to the Internal Network which

>is again not the case in Scenario1 as the traffic is again restricted by the

>dedicated FW.

>

microsoft.public.backoffice.smallbiz2000: Re: Security Issue with ISA and Exchange Front end

>*So can someone who can access these scenarios from a security perspective*
>*give me a feedback as this is of high priority to me...*
>
>*Thanks in advance*
>*regards,*
>*Srini*
>
>

Scenario 1 is a flat no. Don't put an Exchange FE in a DMZ. The ports required between the DMZ and the inside render the DMZ much less secure than it needs to be.

Senario 2 is fine as far as it goes. Use a certificate instead and make OWA available via SSL on tcp 443. Same for POP/IMAP (995/993)

Your risk in Scenario 2 is the lowest, short of not connecting to the Internet at all.

Mark Arnold MCSA MCSE+M MVP, mark@mvps.org
FAQ: <http://www.swinc.com/resource/exchange.htm> &
<http://www.swinc.com/resource/e2kfaq.htm>