

Microsoft Exchange Server Product Support Bulletin

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-02/1361.html>

From: Steven Banks [SBS MVP] (steve_at_newsonline.banksnw.com)

Date: 02/12/04

Date: Wed, 11 Feb 2004 22:34:11 -0800

Got this in an email from Microsoft PSS today and thought I would share it with the rest of you who may not have had the opportunity to have one emailed to you.

Steve

Exchange Security Best Practices:

As part of our commitment to help customers improve and maintain security, Microsoft Product Support Services works to provide proactive information that can help customers implement best security practices.

With the recent activity in mass mailer e-mail worms, we wanted to advice you of some Exchange security best practices that you can use to improve your security and availability.

Specifically, we wanted to let you know of some best practices around:

- . File-level virus scanners
- . Disaster recovery
- . Closing open relays
- . Configuring attachment blocking using Microsoft Outlook

File-level Virus Scanners

When using a "File-Level" virus scanner make sure to exclude the following directories:

- . Exchange 2000/2003:

The Exchsrvr\MDBData and SRS directories on all drives.

. Exchange 5.5:

The Exchsrvr\MDBData and DSADData directories on all drives

File-level scanners scan a file when it is used or at a scheduled interval, and may lock or quarantine an Exchange log or database file while Exchange tries to use the file. This may cause a sever failure in Exchange 5.5 / 2000 / 2003 Server, and may also generate -1018 errors.

Please also pay special attention on your Exchange 2000 servers not to scan the M: drive. File-Level scanning of your M: drive may cause calendar items to disappear from users folders.

The articles listed below should help answer any questions you may have regarding Exchange Antivirus Issues.

<http://support.microsoft.com/?id=328841> – XADM: Exchange and Antivirus Software

<http://support.microsoft.com/?id=298551> – XADM: Large Number of Transaction Logs Created

<http://support.microsoft.com/?id=300608> – XADM: A "C1041737" Error and an Event ID 470 Message May Be Displayed

<http://support.microsoft.com/?id=298924> – XADM: Do Not Back Up or Scan Exchange 2000 Drive M

Exchange Disaster Recovery

Do you need to recover data from a backup (private or public store) and have questions about how to setup the recovery environment or the restore itself? What do you need to setup for Active Directory and DNS? Do you need to have the same Organization, Admin group, Server, and Store names as the production environment?

These articles will help guide you to solutions to these questions:

<http://support.microsoft.com/?id=258243> – How to Back Up and Restore an Exchange 2000 Computer

<http://support.microsoft.com/?id=257415> – Running a Disaster Recovery Setup

<http://support.microsoft.com/?id=241635> – Disaster Recovery Includes Metabase Backup and Restore

<http://support.microsoft.com/?id=313184> – Disaster Recovery of Information Store on Exchange Server

White Paper for Exchange 2003 Disaster Recovery

<http://www.microsoft.com/downloads/details.aspx?FamilyID=df144af6-bee5-4b35-866a-557e25fe2ba1&displaylang=en>

White Paper for Exchange 2000 Disaster Recovery

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6E55DD49-8A6C-4F30-947E-BDE>

White Paper for Exchange 5.5 Disaster Recovery

<http://www.microsoft.com/downloads/details.aspx?FamilyID=df586628-3abe-40c3-8e8f-beb4122de3d7&displaylan>

A best practice in the area of data recovery is to test your backup files monthly and become familiar with the processes itself. Should it ever become necessary to restore data to your production environment, your familiarity with the procedure will lessen the downtime of your servers.

Closing an Open Relay

Top causes for open relays with Microsoft Exchange Server

- SMTP service is live on the internet and not enforcing authentication to relay
- SMTP server has accounts locally or part of a domain that have poor passwords or no password at all.

These articles should help guide you to configuring and preventing your Microsoft Exchange Server from becoming an open relay and how to look for key clues in the future to ensure it doesn't relay.

<http://support.microsoft.com/?id=310380> – HOW TO: Prevent Exchange 2000 from Being Used as a Mail Relay in Windows 2000

<http://support.microsoft.com/?id=324958> – HOW TO: Block open SMTP Relaying and clean up Exchange Server (article can be used with Exchange 2000 and Small Business Server) <http://support.microsoft.com/?id=300580> – Cannot send E-Mail Messages to a growing list of domains

<http://support.microsoft.com/?id=313395> – HOW TO: Examine relay restrictions for anonymous SMTP connections and filter unsolicited E-mail messages in Exchange 2000 Server

Here is a list of known accounts that have potential of being compromised and should either be disabled or should have a strong password. These accounts have been logged in past cases through the event viewer after turning up diagnostic logging. Remember, the passwords should never match the login name.

Webmaster

Admin

Root

Test

Master

Web

www

administrator

backup

server

data

abc

guest

Configuring Attachment Blocking Using Microsoft Outlook

Outlook 2000 (Pre-SP2), Outlook 98 and Outlook 97 Outlook 2000 (Pre-SP2), Outlook 98 and Outlook 97 do not have mechanisms to block attachments. If you are using one of these versions virus/worm protection must be provided on the Exchange Server. It is recommended that you upgrade to Outlook 2000 SP2 to provide this protection for the client.

Outlook 2003, Outlook XP and Outlook 2000 SP2 By default, Outlook 2003, Outlook 2002 (XP) and Outlook 2000 SP2 provide an attachment security feature. This security feature is designed to increase the security protection for certain types of e-mail attachments. This feature provides explicit warning language when attachments are opened, and you have to save the attachment to the file system before opening it. This can help you avoid accidentally releasing viruses that hide in certain file types.

While Microsoft does not recommend reducing e-mail client security levels, there may be instances when an organization wants to customize or remove the additional protections provided by Microsoft Outlook.

You can modify default security settings for the Microsoft® Office Outlook® client by using the Outlook Security template, which you install as a form in Outlook. To implement this see the following article:

<http://support.microsoft.com/?id=290499> – OL2002: Administrator Information About E-Mail Security Features

Other related articles and resources:

<http://support.microsoft.com/?id=290497> – OL2002: You Cannot Open Attachments Customizing Security Settings by Using the Outlook Security Template <http://www.microsoft.com/office/ork/2003/three/ch12/OutG03.htm>

Closing

We hope this information is helpful as you work to implement security to protect against mass mailer e-mail worms.

Should you have additional questions regarding this information please contact Product Support Services. Methods for contacting Product Support Services can be found at the following location:

[http://support.microsoft.com/default.aspx?scid=sz;\[ln\];top](http://support.microsoft.com/default.aspx?scid=sz;[ln];top)

--

Banks Consulting Northwest

<http://www.banksnw.com>