GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

# Securing Microsoft Exchange 5.5

by Michael Sneddon

**Secure the NT server**

When considering the security of an Exchange 5.5 server, it is very important to remember that Exchange is living on a server that has its own security requirements. So, the best starting point for securing Microsoft Exchange 5.5, is securing your server installation. Without securing the core installation of your server, every other step you take to secure Exchange may be pointless. Microsoft provides assistance in securing your server installations with the **Windows NT 4.0 Member Server Configuration Checklist**[1], the **Windows NT 4.0 Domain Controller Configuration Checklist**[2], or the **Windows 2000 Security**[3] white paper. Securing a server is an extensive undertaking in its own right, so that process will not be detailed here. Always remember that Exchange is not secure if the server it resides on is not secure.

**Exchange 5.5 Shared Directories**

With the NT 4.0 installation secured, you can now focus on securing the installation of Exchange 5.5. During the installation of Exchange 5.5, shared directories are created for other Exchange servers within the site. Microsoft's position is that "Setup sets permissions for these directories that are usually sufficient for most organizations."[4] Depending on your environment and the level of security required for your Exchange server, you may want to alter the permissions on these shared folders. When changing permissions on the shared Exchange directories, be extremely cautious, since a minimum level of permissions are required for the normal operation of Exchange.

The shared directories created by the Exchange setup are Add-ins, Address, Connect, Connect\Msmcon\Maildata, Res, and Tracking.log. The group Everyone is given READ permissions to all of the shared directories, plus FULL CONTROL permissions for the Maildata directory. The Exchange service account and the local Administrators group are given FULL CONTROL permissions to all of the shared directories.

If you determine that you need a higher level of security on these folders, there are a few guidelines to follow. Permissions for the group "Everyone" can be removed from all of the shared directories and replaced with the accounts of specific administrators assigned to various administrative duties. For example, the Tracking.log directory contains message specific information that should only be accessible to administrators with responsibility for tracking mail messages. The Maildata directory only needs to be accessible to administrators that are responsible for the Microsoft Mail Connector. All other administrators can be given permissions to the Add-ins, Address, Connect, and Res directories. The biggest caution in making changes to these directories involves the permissions for the Exchange service account and the local Administrators group. Do not change the permissions for the service account or the local Administrators group, since this will greatly affect the fundamental operation of the Exchange server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Install Service Packs**

Just as it is important to maintain the latest Service Pack levels on the operating system, it is equally important to install the latest service pack for Exchange. As of this writing, Microsoft lists Service Pack 4 (SP4) as the most current Service Pack. Service Pack 4 is a release that includes all updates to Microsoft Exchange 5.5 including all the Microsoft Quick Fix Engineering patches and all of the fixes, utilities, and enhancements that were included in Service Pack 3 for Exchange 5.5. Microsoft has issued a number of security bulletins addressing Exchange 5.5 security problems. Listed, are the Service Packs and the vulnerabilities that Service Pack first repaired.[5]

Service Pack 4

Q275714 – XADM: Information Store Stops Unexpectedly with Multipart or Mixed Message and Null Boundary String

A malicious user could cause an Exchange server to fail by providing a particular type of invalid MIME value in the MIME header fields.

Service Pack 3

Q237927 – XIMS: Messages Sent to Encapsulated SMTP Address Are Rerouted Even Though Rerouting is Disabled

A malicious user could produce a Denial of Service Attack by over utilizing Exchange server resources for mail relaying and could generate unauthorized mail with a disguised point of origin.

Q221989 – XADM: Buffer Overrun in Exchange Server 5.5 LDAP Service

This vulnerability could allow a Denial of Service attack triggered by a malformed Bind request that overflows the buffer thereby causing the Exchange Directory service to crash. Certain buffer overrun techniques could also cause arbitrary code to be run on the Exchange server.

Service Pack 1

Q188341 – XFOR: Auth and EHLO Command Cause Internet Mail Service to Stop

Exchange's processing of incorrect Auth and EHLO commands can generate an application error that stops the Internet Mail Service. Restarting the Exchange services will make the Exchange server operational again.

Not Corrected by Exchange Service Packs

Q217004 – BackOffice Installer Tool Does Not Delete Password Cache File

If Exchange 5.5 was installed using the BackOffice Installer V.4.0, user account and password information is stored in a reboot.ini file that remains after the installation has completed. A user that has the ability to log on locally to the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

server and can access the Program Files\Microsoft BackOffice folder could then obtain the information from the reboot.ini file. To eliminate this vulnerability, the system administrator should delete the reboot.ini file.

Q148427 – Generic SSL (PCT/TLS) Updates for IIS and Microsoft Internet Products

SSL encrypted transactions can be decoded by recording an initial SSL transaction and then repeatedly sending messages to the Exchange server which generates responses that the malicious user could then use to decode the recorded transaction. Besides making encoded data vulnerable, the Exchange server will experience degraded performance due to the numerous messages and responses being handled. NT 4.0 Service Pack 4 corrected this problem. The problem is not specifically an Exchange issue but rather an IIS problem that may impact certain installations of Exchange.

**Key Management Server**

The Key Management server (KM server) component is not installed by default during the standard installation of Exchange. Installing KM server allows you to take advantage of public and private key encryption. If you haven't installed Service Pack 1 for Exchange 5.5, you are limited to the standard KM server, which only supports certificates for Outlook clients. If Service Pack 1 or higher for Exchange 5.5 is installed, you can use Microsoft Certificate Server to generate certificates that are compatible with all clients that follow the S/MIME standard.

The KM server needs to be installed on an Exchange server. The following security and performance guidelines should assist in choosing the server that should host the Key Management Server:

- The physical location of the server should be secure.
- Key Management Server must run on the same machine as an Exchange Server. Pick an Exchange server that will be in place for a long time; moving KMS to another server is a pain in the neck.
- From the network's perspective, the Exchange server that hosts Key Management Server should be in close proximity to the Exchange security administrator. The administrator must be able to connect to this server using an RPC connection.
- Though Exchange Server 5.5 permits more than one Key Management server per Exchange organization (Exchange 4 and 5 did not), you should keep the number of KMS servers to a minimum. You are still limited to a single KMS per site.[6]

Installing the KM server requires the Exchange Server 5.5 CD and the Exchange service account and password for your site. The KM server installation option can be selected during the initial installation of Exchange using the following steps:

1. During the Exchange Server 5.5 setup, choose the Custom installation option.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. Highlight the Microsoft Exchange Server option and click the Change Option button.
3. Make sure that the Key Management Server option is selected.
4. Click "OK" and "Continue" to begin the installation of the Exchange Server (and KM server software). [7]

For administrators that have already installed Exchange Server 5.5 and now want to add KM server, a couple of major points must be considered. First, running the Exchange setup and choosing the Add/Remove option will allow you to install the KM server software, but you will have to stop the Exchange services, which will force all of your users out of the mail system. Second, since the installation of the KM server is run from the original Exchange CD, any Exchange service packs and hot fixes will have to be reapplied before restarting the Exchange services.

Regardless of when you install the KM server, during the original installation of Exchange or later on, make sure you note the KM server password that is generated for you. This password is required to start the KM server service. If you lose this password the KM server service cannot be started and your only choice would be to reinstall the KM server. A reinstall of the KM server would result in all of the current keys being lost as the key database is overwritten. During installation, the password can be displayed on the screen and recorded, or you can have the password written to a pair of disks. If you display the password, realize that the only way to start the KM server service is by manually entering the password. If you chose to write the password to disk, one disk must be in the floppy drive when the KM server service starts. The other disk is your backup copy of the password. Always remember to start the KM service when you reboot the server. The service is automatically set as a manual service and you won't be prompted to start it. If you displayed the password during the installation, you must enter it as a start parameter within the services applet before you press the "Start" button. If you forget to start the KM server service, clients will still be able to send and receive encrypted messages, you just won't be able to create, revoke, recover, or renew certificates.

Once you have installed the KM server you can generate public and private encryption keys. The KM server will also function as a Certificate Authority, creating public signing certificates as well as X.509 certificates. An important note here is that each time you open the Certificate Authority object, you will be prompted for the KM server service password. After the KM server has generated the public and private keys and the certificates, this information is distributed to the client computers. This allows client computers to send and receive encrypted and signed messages even if the KM server is down or the client is not attached to the network.

To help in administration of the private encryption keys, the KM server maintains a copy of each key in an encrypted database. The encrypted database allows administrators to read encrypted mail for employees that have left the company, to replace the .epf security file and registry settings related to the private key, and to assist users that have forgotten their security file password. Finally, the KM server keeps a Certificate Revocation List

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

to prevent the use of compromised certificates. The KM server will distribute a replica of the revocation list to client computers to guarantee that certificates are being checked even when the computer is offline.

KM server provides Exchange the added level of security provided by encryption. Public key cryptography is used by Exchange to verify digital signatures. If the public and private keys correspondingly match, signatures are considered to be valid. By comparing checksums created at the time the message was signed and checksums on the plain text message, Exchange verifies that messages have not been modified since the time they were signed and sent.

Microsoft has provided multiple encryption types based on the security needs of your organization and the type of mail clients that are being used. Those who require strong encryption should use either DES or CAST 64. Due to U.S. export regulations, international users are limited by the International version of the Outlook client to CAST 40 encryption. Exchange sites that span more than one country can mix and match encryption types. Exchange maintains information about the type of encryption supported for each user in the organization and will choose the appropriate encryption to encrypt each message. One thing to consider is that when a message is sent to multiple recipients, the encryption type chosen will be the one that all users share. Because of this, you may end up with a message that is not encrypted as strongly as you believed. If you have users that are not using encryption security at all, you can choose not to send the message to those users, or you can have the message sent as plain text.

**SMTP Mail Relay**

In securing your Exchange server, you will also want to prevent malicious users from utilizing Exchange's SMTP mail relay capability to send unauthorized mail using your server. Unauthorized Commercial E-mail (UCE), more commonly known as spam, can be generated by relaying messages through an unprotected Exchange server in order to hide the real origin of the message. If you are using the Internet Mail Connector you will want to make changes to the properties of the Internet Mail Service to prevent mail relaying. This can be accomplished with the following steps:

1. Open the Exchange Administrator program.
2. Expand the site that contains the Internet Mail connector.
3. Expand "Configuration."
4. Open "Connections."
5. Open the Internet Mail Service.
6. Select the "Routing" tab.
7. Select the "Do not reroute incoming SMTP mail" radio button.
8. Click OK to close the IMS properties dialog.
9. Stop the IMS.
10. Start the IMS.

Just turning off Exchange's ability to reroute incoming SMTP mail may not fully meet your requirements to prevent the use of your mail server to relay SMTP messages. While

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the relaying has been prevented, systems configured in this manner still accept messages and generate non-delivery reports. Because of the acceptance of the messages and the subsequent generation of the non-delivery reports, Exchange servers running the IMS that have had relaying disabled, may suffer performance hits while processing relay attempts.

> "In February 1999, the IETF released RFC 2505, "Anti-Spam Recommendations for SMTP MTAs." This RFC explains the problems associated with unsolicited commercial email (UCE, or spam) and specifies the functionality that an SMTP Message Transfer Agent (MTA) needs to reduce UCE's effects. RFC 2505 makes 13 recommendations, two of which are most closely related to relaying:"
>
> - A system must be able to restrict unauthorized use as a mail relay.
> - A system must be able to configure and provide different return codes for different rules (e.g., 451 Temp Fail vs. 550 Fatal Error). Specific return codes let you diagnose configuration problems that are blocking legitimate mail delivery.[8]

Setting up Exchange to "Do not reroute incoming SMTP mail," meets the first requirement of the RFC, but fails the second requirement, because the non-delivery report indicates that the mail was accepted and not delivered rather than rejected. Even worse, the fact that a non-delivery report is generated, can be used by the malicious user to relay mail utilizing "reverse UCE." By falsely setting the Sender's Address as the intended recipient's address and by setting the recipient address to fail, all of the messages will be relayed to the intended recipients as non-delivery reports. In this way, a system that was set to not relay mail has just relayed messages to any recipient the malicious user has chosen and the source of these messages is your server. To prevent this situation, you must use another IMS option.

Instead of choosing "Do not reroute incoming SMTP mail," configure your Exchange server to reroute mail appropriately.

1. Open the Exchange Administrator program.
2. Expand the site that contains the Internet Mail connector.
3. Expand "Configuration."
4. Open "Connections."
5. Open the Internet Mail Service.
6. Select the "Routing" tab.
7. Select the "Reroute incoming SMTP mail (required for POP3/IMAP4 support)" radio button.
8. Press "Add…" to enter your primary mail domain and any domains that you host mail for.
9. Configure the domain to "Should be accepted as inbound" and click OK.
10. Press the "Routing Restrictions…"
11. Select the "Hosts and clients with these IP addresses" check box but not specify any IP addresses and click OK.
12. Click OK to close the IMS properties dialog.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

13. Stop the IMS.
14. Start the IMS.

What you have done is change the way that Exchange handles messages. Now the Internet Mail Service will check messages before they are accepted. If the message is not intended for local delivery, a "Relaying Prohibited," message is returned. So, instead of allowing the system to accept messages and return non-delivery reports, the messages are stopped before they are processed and the use of reverse UCE is prevented.

**Additional Steps**

In order to create a secure environment there are additional items that should receive attention. Some are very obvious, like making sure that you have anti-virus software for Exchange. Some are easily overlooked, like making sure your Outlook clients for Exchange are secured because "in the process of securing Exchange email clients, you must protect two types of assets: logon credentials and message data."[9] Also, don't limit yourself to Microsoft solutions. Many additional security and encryption products are available for Exchange from third-party solutions providers (See list at http://www.amrein.com/eworld.htm ) Just as we do with all security, remember to practice "defense in depth." Never rely on a single fix or technique to protect your mail data. Implement as much security as you can without compromising the usability that is expected of today's e-mail systems. Exchange 5.5 is not secure by default, but with a little attention, you can start to build the "defense in depth" that you need to protect your e-mail data.

**References**


[1] Microsoft Technet. "Windows NT 4.0 Member Server Configuration Checklist." Microsoft Technet Security. June 6, 2000 URL: http://www.microsoft.com/technet/security/mbrsrvcl.asp (17, January, 2001)

[2] Microsoft Technet. "Windows NT 4.0 Domain Controller Configuration Checklist." Microsoft Technet Security. March 29, 2000 URL: http://www.microsoft.com/technet/security/dcchklst.asp (17, January, 2001)

[3] Microsoft Technet. "Windows 2000 Security." Microsoft Technet Security. November 22, 2000 URL: http://www.microsoft.com/technet/security/wn2ksec.asp (17, January, 2001)

[4] Microsoft Press. Microsoft Exchange Server 5.5 Resource Kit. Redmond, Washington: Microsoft Press, 1999, p. 270 e

[5] Microsoft Technet. "Security Bulletin Search." Microsoft Technet. January 17, 2001 URL: http://www.microsoft.com/technet/security/current.asp?productID=4 (17, January, 2001)


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[6,7] Mcbee, Jim. "Exchange Server Advanced Security." Chapter 14 from *Exchange Server 5.5, 24 seven*, published by Sybex Inc. June, 16, 2000 URL: http://wwww.microsoft.com/technet/security/advan.asp#a (17, January, 2001)

[8] Neubauer, Joseph. "Is Your Exchange Server Relay-Secure?" Exchange Administrator. January, 2000 URL: http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=7696 (22, January, 2001)

[9] Sakellariadis, Spyros. "Using Exchange Clients Securely" Windows 2000 Magazine. October, 1998 URL: http://www.win2000mag.com/Articles/Index.cfm?ArticleID=3847 (22, January, 2001)

© SANS Institute 2000 - 2002, Author retains full rights.