Hardening Exchange Server 2007 – Part III

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this small article series I will show you how to harden an Exchange Server 2007 environment with SP1 (Beta), installed on Windows Server 2008 (also Beta) as I wrote these articles. We will talk about the necessary steps how to harden the underlying operating system by only installing a minimal number of server roles and services. This is the last article of this small article series and will explain how to secure client access from OWA, POP3/MAP4 and Outlook Anywhere.

Let's begin

Before we begin, please note that this article is based on a beta version of Windows Server 2008 and Exchange Server 2007 SP1 and it is possibly that some features will be changed or removed in the final versions of these products.

First, I do not want to write the same things that Rui Silva wrote in his article series about Hardening Exchange Server 2003 here at www.msexchange.org, so that I tried to only write some new things especially to Exchange Server 2007 and Windows Server 2008. If you want to find additional information about securing the environments, educating user and much more, I recommend reading his articles.

In this last article I will give you a high level overview about securing different e-mail client types such as POP3, IMAP4, OWA and Outlook Anywhere (also known as RPC over HTTP(S).

POP3

POP3 (Post Office Protocol version 3) is a relative old protocol to get e-mails from an e-mail server like Exchange Server. Beginning with Exchange Server 2003, Exchange supports using POP3 but the protocol is disabled by default. The same is true for Exchange Server 2007, so you must change the startup type of this protocol to Automatic. One of the important changes in Exchange Server 2007 POP3 access is that no unencrypted sessions are allowed. Exchange Server 2007 uses a self signed certificate to secure the message transmission. As a result you have to configure your e-mail client to access the Exchange Server over a secure connection. It is a goof idea to remove the self signed certificate after the Exchange installation with a trusted certificate from an inhouse Certificate Authority or with a certificate from a trusted third party CA (Certificate Authority). As you might know, to configure POP3 access, you must use the Exchange Management Shell (EMS). Beginning with Exchange Server 2007 SP1 parts of managing POP3 will be part of the Exchange Management Console (EMC).

IMAP4

IMAP4 (Internet Message Access Protocol version 4) is a relative old protocol to get e-mails from an e-mail server like Exchange Server. IMAP4 is the successor of POP3 with several enhancements.
Beginning with Exchange Server 2003, Exchange supports using IMAP4 but the protocol is disabled by default. The same is true for Exchange Server 2007, so you must change the startup type of this protocol to Automatic. One of the important changes in Exchange Server 2007 IMAP4 access is that no unencrypted sessions are allowed. Exchange Server 2007 uses a self signed certificate to secure the message transmission. As a result you have to configure your e-mail client to access the Exchange Server over a secure connection.

Ports used by POP3 and IMAP4

Protocol	Default port
IMAP4/SSL	993 (TCP)
IMAP4 with or without TLS	143 (TCP)
POP3/SSL	995 (TCP)
POP3 with or without TLS	110 (TCP)

OWA

Outlook Web Access (OWA) is also secured per default. As any other Exchange client services, Outlook Web Access is also secured with a self signed certificate and the HTTPS access is activated per default. It is recommended that Administrator uses its own certificate for OWA access from a trusted internal Certificate Authority (CA) or from a trusted third party CA. Exchange Server 2007 Outlook Web Access provides some additional security settings. Some of these security settings are part of the additional Outlook Web Access security package which was first introduced with Exchange Server 2003. Most settings of this tool (and some additional more) are now available native in Exchange Server 2007. Exchange Server 2007 provides this additional security feature:

- Outlook Web Access segmentation
- Outlook Web Access Full feature client and light version
- Restrict access to Outlook Web Access for specific users
- Customizing Microsoft Office Sharepoint Integration
- Controlling Direct Access to file Server shares
- Block access for specific file types

Outlook Anywhere

Outlook Anywhere, formerly known as RPC over HTTPS in Exchange Server 2003 provides full Outlook 2007 access over HTTPS from outside the internal network. Because securing Outlook Anywhere is similar to OWA, I wouldn’t write more here about this feature.

Exchange Active Sync (EAS)

Exchange Active Sync provides access to e-mail and more for mobile clients like Smartphones, PDAs (Personal Digital Assistants) and mobile phones. EAS is activated by default and it is possible to configure EAS settings with Exchange Active Sync policies. With the help of policies you can enforce the following settings:

- Request passwords for mobile clients
- Request alphanumeric password
- Allow or disallow downloading of attachments
- Allow access to Windows Sharepoint services documents
- Allow the wiping of stolen or lost devices
- Activate device encryption

ISA Server 2006

You can use ISA Server 2006 (Internet Security and Acceleration Server) to provide an additional Layer of security for accessing Exchange Server 2007 with Outlook Web Access (OWA), Outlook Anywhere and Exchange Active Sync (EAS). With the help of ISA Server 2006 you can securely publish all these Exchange Server clients. ISA Server 2006 provides additional security in form of HTTPS to HTTP Bridging, Link Inspection, Content filtering, user pre authentication and many more.

Patch Management

It is important to keep your Messaging clients and the underlying operating system up to date. You should use WSUS (Windows Server Updates Services) or other patch Management software.

AntiSPAM

Exchange Server 2007 can use integrated AntiSpam features for the Hub Transport Server role and the Edge Transport Server role.
You must activate the AntiSpam features on a Hub Transport Server via the Exchange Management Shell (EMS).
Exchange Server 2007 provides the following AntiSpam feature:

- Aggregation of Outlook Junk E-mail Filter Lists
- IP Reputation Service
- Sender reputation
- Sender ID
- Recipient filtering
- Spam quarantine
- Content filtering
- Connection filtering
- SMTP Tarpitting

You can use Forefront Edge Security to provide some additional AntiSpam features.

AntiVirus

You should use a client side AntiVirus scanner which scans file access on demand like Forefront Client Security. On Server site you should use a central AntiVirus solution like Microsoft Forefront Edge Security as mentioned in the second part of this article series.

Conclusion

In this third and last part of this small article series we discussed how to secure client access from various clients like POP3, IMAP4, OWA and Outlook Anywhere. Please note that this article could not focus all security enhancements and new security features of Exchange Server 2007.

Links

Exchange Server 2007 – Security and protection
http://technet.microsoft.com/en-us/library/aa996775.aspx
Securing Exchange Server 2007 Client Access
http://technet.microsoft.com/en-us/library/bb400932.aspx
Hardening an Exchange Server 2003 Environment (Part 1)
http://www.msexchange.org/tutorials/Hardening-Exchange-Server-2003-Environment-Part1.html
Hardening an Exchange Server 2003 Environment (Part 2)
http://www.msexchange.org/tutorials/Hardening-Exchange-Server-2003-Environment-Part2.html
Hardening an Exchange Server 2003 Environment (Part 3)
http://www.msexchange.org/tutorials/Hardening-Exchange-Server-2003-Environment-Part3.html
Hardening an Exchange Server 2003 Environment (Part 4)
http://www.msexchange.org/tutorials/Hardening-Exchange-Server-2003-Environment-Part4.html
Introduction to Exchange 2007 Server Roles
http://www.msexchange.org/tutorials/Introduction-Exchange-2007-Server-Roles.html
Microsoft Forefront
http://www.microsoft.com/forefront/default.mspx
Using POP3 and IMAP4 to Access Exchange 2007
http://www.msexchange.org/articles_tutorials/exchange-server-2007/mobility-client-access/using-pop3-imap4-access-exchange-2007-part1.html
http://www.msexchange.org/articles_tutorials/exchange-server-2007/mobility-client-access/using-pop3-imap4-access-exchange-2007-part2.html
Microsoft Internet Security and Acceleration Server 2006
http://www.microsoft.com/isaserver/default.mspx