Global Information Assurance Certification Paper

Antivirus Solutions for Microsoft Exchange 2003
Scott Palmer
GIAC Certified Windows Security Administrator (GCWN) Practical Assignment
Version 5.0, Option 1: Solving a Windows Problem
January 27, 2005

Abstract

The Microsoft Exchange Server email system has many issues that involve security. The lack of built-in virus protection is perhaps the most apparent of these current security issues. Microsoft has gone to considerable effort to develop an API (application programming interface) to enable third party antivirus vendors to integrate their products with Exchange Server so that proper protection of information store can be provided.

This paper will attempt to outline the features of an ideal antivirus solution for Exchange Server, compare three products and provide an installation guide and configuration tips for one of the products.

Introduction

In a recent Server Watch (http://www.serverwatch.com) article Aaron Weiss wrote: “E-mail has long been considered the "killer app" of the Internet. Some 12 trillion e-mail messages are estimated to be sent around the globe every year — and that figure alone grows by the day.” [1] The intended meaning of the term “killer app” in this article is that email is the defining and sustaining application that has helped Internet become as popular as it is today. However, due the threats of various types of malware that can be transmitted via email, it could very well be the app that kills a business connected to the Internet if proper precautions are not taken.

Due to the ever-growing and changing risks that viruses and worms pose to network security, it has become common practice to implement a multi-tier or leveled antivirus regiment to protect against these threats. Typically 3 levels of defense are used in this antivirus model. The first level is at the firewall or gateway. This level should perform at least SMTP virus protection. Ideally HTTP (detecting ActiveX and Java malware), POP3 and FTP scanning should also be performed at the firewall or gateway level. Sometimes virus diction at this first level is referred to as “edge virus scanning.” The second level of virus protection should be implemented on all servers in a network. The third and last level of virus protection is implemented on the desktop/client itself. It is best if this third level not only provides real-time virus protection of the client operating system but also integrates with the email client. Ideally all three levels of protection should be provided from different antivirus vendors to attempt to maximize the strengths of their different pattern matching and heuristic engines and virus definition updates. By implementing this 3 layer virus protection

model, defense in depth should be achieved.

Specialized products are designed for each tier of defense for this three level virus protection strategy with their functionality dictated by the specific objectives of protecting that layer. In the second tier or layer, servers running email systems need virus protection products that are explicitly designed to protect the databases that email messages are stored in. Although it would be an interesting study to compare a product from each of the three tiers or layers described, I felt it would be more productive to compare three products designed for the exact same purpose. This paper will focus on the second tier or level, providing virus protection for the information store of the Microsoft Exchange Server email system. By considering only this single part of the multi-tier model, a more detailed analysis could be conducted of products that are designed to perform the exact same function.

Section 1: Describe a Security Issue on Windows Platform

According to a white paper on corporate messaging analysis published The Radicati Group, Inc. in June of 2004, Microsoft Exchange Server has 31% of the market share. [2] In a different article published in June 2003 by Directions on Microsoft, Exchange Server's market share is describe as "the dominant corporate e-mail server" and has "roughly 50% market share in terms of mailboxes served." [3] In the absence of the exact the market share percentage that Microsoft Exchange Server possesses, it cannot be argued that it is the most popular email system in use today in Windows environments. Exchange Server's popularity is most likely due to the incredible email and groupware functionality, the easy installation and management and the improvements that Microsoft has made in past versions and are planned for the future. However for all of Exchange Server strengths, it does have a few areas that it falls short. The protection from email viruses is one glaring area where Exchange Server lacks a built-in security solution.

Exchange Server was not originally designed to protect against virus infections. This oversight is most likely because in 1996, the time of Microsoft Exchange Server 4.0's release, the threats to email that are so prevalent today did not exist or were considerably more remote. As the threat of malware contained in email has developed, Microsoft has made a concerted effort to build into the Exchange Server product tools to help third parties produce anti-virus products. Portions of the following discussion of antivirus APIs included in Exchange Server heavily rely on information from a Microsoft Webcast given on May 26, 2004. [4] Initially antivirus companies had to use MAPI (Mail Application Programming Interface that email clients use) or replace the driver for the Extensible Storage Engine in order to protect an Exchange Server information store. Both of these solutions have serious drawbacks. MAPI virus scanners are very inefficient and are not guaranteed to scan an email message before the recipient opens it. MAPI virus scanners can also not scan outbound

email. Microsoft does not support the Extensible Storage Engine scanners because of the nature of replacing a portion of Microsoft's code for Exchange Server. In Exchange Server 5.5 Service Pack 3, Microsoft introduced VAPI 1.0, the Virus scanning Application Programming Interface (also referred to as VSAPI). This library provided antivirus vendors with links into Exchange Server so that email could be properly scanned whenever a message is accessed by a client. VAPI 2.0 was introduced in Exchange 2000 Service Pack 1. VAPI 2.5 was introduced with Exchange 2003. Improvements in VAPI have mainly been in priority handling. VAPI 2.0 added the ability for antivirus vendors to proactively scan email messages rather than just when an email was accessed. A low priority is assigned to messages arriving to the Exchange Server and elevated to high priority if a user attempts to access the message. VAPI 2.5 main enhancements deal with transport scanning which allows emails to be scanned not destined for the local Exchange Server. This transport scanning is used for Exchange Servers in a gateway or bridge head roles. VAPI 2.5 also added better virus status messaging so clients can be made aware of more specific details on a message.

Due to the advanced capabilities of Exchange Server which allow any type of attachment in email messages, Public Folders and the Installable File System which allows mailboxes to be accessed just like part of a network file system viruses and worms are a serious threat. The security implications of doing nothing and not taking preventive action against the risk of email viruses are staggering. The possibility of monetary loss is the largest threat from inaction. A virus or worm outbreak could drastically affect the availability and integrity of an email system. Data loss could have devastating effects on an organization. Substantial downtime of an email system can also damage an organizations public image. Some viruses attempt to email files located on network files share which could lead to embarrassing confidentiality issues or again monetary loss if trade secrets or strategic information is revealed. Finally, some businesses face regulatory requirements to retain email for specific lengths of time and also to show reasonable efforts to insure security of their networks and emails systems. Again, monetary loss via fines from regulatory agencies could be imposed if adequate precautions aren't taken to secure a businesses email system. Considering these issues, protecting your enterprises email system with some form of anti-virus protection is not an issue of convenience but a security requirement.

An optimal tool for protecting an Exchange Server's information store would have all of the following features:

- VAPI 2.5 compatibility
- Timely virus definitions releases and flexibility to configure frequent attempts to get updates.
- Real-time protection of group folders/mailboxes/SMTP Transport protection
- Manual and scheduled scanning
- Content filtering and dangerous file type blocking
- Quarantine functions

- Wide range of notification capabilities
- Excellent management tools

Section 2: Product Evaluation

Narrowing the choices for comparison

There are numerous antivirus vendors offering products that provide integrated Exchange Server virus protection. Microsoft lists about 20 partners that provide antivirus products on their website at the following URL: http://www.microsoft.com/exchange/partners/antivirus.asp Another list of antivirus products designed for Microsoft Exchange Server protection is at the following URL: http://www.msexchange.org/software/Email-Anti-Virus/ The task of trying to select which antivirus product to use out of all the choices seems daunting. In an attempt to select three products to evaluate, I considered an eWeek article by Larry Seltzer where he makes an interesting comment about considering the size of the company that provides your antivirus solution:

"…the larger security companies have a genuine advantage in their ability to respond to new threats. When I see malware protection from little companies or even looser affiliations, I don't get a warm fuzzy about their ability to respond quickly." [5]

This quote expresses an opinion that some people may not agree with. Antivirus products tend to create a dedicated consumer base that enthusiastically defends the merits of the product that they use. I decided to disregard any controversy and used the size of the antivirus vendor as a major point in my selection criteria. Also, I considered Microsoft's acquisition of the antivirus firm GeCad in 2003 (see Microsoft Press Release [6]), its recent release in January 2005 of the Microsoft Malicious Software Removal Tool which it promises to update the second Tuesday of every month and the release of the Microsoft Exchange Intelligent Message Filter. It does not take considerable imagination to see Microsoft releasing its own antivirus products and especially adding virus protection to the Intelligent Message Filter itself. If this happens, I would expect to see some market consolidation take place with the smaller antivirus companies disappearing. The lack of an open source solution that provides integrated Exchange Server support also helped me narrow my choices to the three market leaders in the antivirus industry: McAfee, Symantec and Trend Micro.

The three products selected for evaluation are McAfee GroupShield 6.0 for Microsoft Exchange, Symantec Mail Security for Microsoft Exchange 4.6 and Trend Micro ScanMail 6.2 for Exchange.

Testing Method Used

In order to evaluate each of the three products, Microsoft Virtual PC 2004 SP1 was used. A virtual machine was constructed with Microsoft Windows

2003 Server (fully patched to current) as the operating system running as a stand alone domain controller. Microsoft Exchange Server 2003 SP1 (fully patched to current) was also installed on this virtual machine. Outlook Web Access was used for the email client. The same virtual machine was cloned and used for the testing of each Exchange Server antivirus solution. The Eicar (http://www.eicar.org/anti_virus_test_file.htm) virus test string was used to test virus protection functionality in the form of COM, TXT, ZIP, nested ZIP and password protected zip files. Please note that due to the nature of Virtual PC and virtual machines providing an accurate measurement of performance was impossible and was not one of the criteria used to evaluate these products.

Comparison Points

Each of the three products evaluated in this section contain a great deal of functionality. Instead of running through the features of each product separately, I thought it would be more productive to structure this section on the eight points previously covered in the ideal antivirus solution for Microsoft Exchange Server. The following documents were heavily used as references for the capabilities and operations of the products reviewed: McAfee GroupShield 6.0 for Microsoft Exchange Installation Guide [7], Symantec Mail Security for Microsoft Exchange Implementation Guide (for version 4.5) [8] and Trend Micro ScanMail 6 for Microsoft Exchange 2000 and 2003 Getting Started Guide. [9]

1. VAPI 2.5 Compatibility

It is critical for an antivirus solution for Microsoft Exchange Server to be compatible with VAPI 2.5. The features of VAPI simply make using another type of technique to protect an Exchange Server's information store obsolete. Antivirus products using VAPI 2.5 are able to scan messages on access, on demand, in the background, on arrival and at the transport layer.
A products compatibility with VAPI 2.5 shows a dedication from the software vendor that they are committed to keeping up with the advances Microsoft is making and an interest in offering the best quality protection they can. All three of McAfee's GroupShield, Symantec's Mail Security and Trend Micro's ScanMail are compatible with VAPI 2.5. It should also be noted that all three products evaluated are also backward compatible with VAPI 2.0 and Microsoft Exchange 2000 Service Pack 1.

2. Timeliness of Antivirus Definitions/Frequency of updates

The timeliness and availability of virus definition updates is very important. If an antivirus solution can't detect a new virus and the defined policies and rules don't stop it then email system is vulnerable. All three of McAfee, Symantec and Trend Micro issue updated virus definition very week. During an outbreak of a new threat of medium risk, each vendor will issue emergency releases of their updated virus definitions. Trying measure which vendor is the first to identify a new virus or variant and then issue an updated definition file to detect it is very difficult. The problem is that the different vendors call viruses and their variants by different names. One can be

reasonable assured that McAfee, Symantec and Trend Micro, who are the top three market leaders in the antivirus industry, are some of the best at detecting viruses and getting updated definitions out quickly. The other part of this puzzle of keeping current with the newest virus definitions is how frequently you can configure the antivirus product to attempt to retrieve new definitions. It was not long ago that antivirus vendors attempted to limit the number of times a month or day their software products would try to retrieve virus definitions in order to prevent their FTP servers from becoming overloaded. With the increase in virus and worm threats, antivirus vendors have had to abandon this practice of limiting update attempts and add capacity to handle an extremely large number of clients trying to update virus definitions during an outbreak. All three of McAfee's GroupShield, Symantec's Mail Security and Trend Micro's ScanMail allow for automatic virus definition updates as frequently as once every hour. Finally each of McAfee, Symantec and Trend Micro have their own research and support center groups. They maintain virus info centers with virus encyclopedias on their websites. Here's a list:

Virus info centers on websites:
McAfee – Avert http://www.mcafeesecurity.com/us/security/vil.htm
Symantec – AVCenter http://www.symantec.com/avcenter
Trend – Trendlabs http://www.trendmicro.com/vinfo

3. Real-time Protection Group Folders/Mailboxes/SMTP Transport protection

Real-time protection of the information store is really the most basic and critically important feature of an antivirus program designed for Exchange Server. The VAPI 2.5 allows for an application to scan messages whenever they are access with high priority and when they arrive with low priority. All three of McAfee's GroupShield, Symantec's Mail Security and Trend Micro's ScanMail provide real-time antivirus protection for an Exchange Server. All three products are also careful to scan an email going to multiple recipients one. Each product has their own technology (and name to go with it) for their scan engines but they are basically just performing pattern matching against virus definition files and heuristic based scans. All three programs are capable of scanning at the SMTP transport layer so they can be used for Exchange servers in bridgehead and gateway roles. One interesting feature of Trend Micro's ScanMail is that it's configurable which (in the event of multiple on an Exchange server) information stores it scans. It is possible to configure ScanMail so that only some information stores are scanned on a server. ScanMail also has a very helpful real-time monitor application that keeps administrators apprised of the applications status.

4. Content filtering and dangerous file type blocking

Although content filtering may seem like a feature that belongs in a separate product from an antivirus solution, it provides essential functionality in stopping virus outbreaks. During mass-mailing worm outbreaks, some administrators configure their email servers to clean infections and send

messages. A large number of emails that once contained a virus, but now only contain the text of the mass-mailing worm are still delivered. Content filtering can be used to automatically delete these unwanted emails if just a small part of the text of the body of the email is known. McAfee's GroupShield 6.0 and Symantec's Mail Security for Microsoft Exchange 4.6 both contain highly configurable content filtering capabilities. These customizable content filtering policies could be used in conjunction with Microsoft's Internet Message Filter to provide a very good antispam solution. It should be noted that the vendors of all three products evaluated have add-ons to add antispam capabilities for an additional charge. Content filtering can provide a vital role within an organization by monitoring for inappropriate, offensive, obscene and confidential material.

Dangerous file type attachment blocking is a critical feature that an antivirus solution for Exchange Server must have. The ability to block executables, scripts and non-business related files types (for example MP3s and AVIs) and prevent unauthorized content from entering your network is critical. All three programs evaluated have the ability block desired file types.

5. Manual and Scheduled Scans

The ability to perform manual and scheduled scans of an Exchange Server information store is very important. Although real-time scanning is occurring on all incoming, outgoing and accessed messages, it is possible that a message containing an undetected piece of malware could be saved into a mailbox or group folder. It's wise to schedule scans of all mailboxes and folders periodically as new virus definition files may become available that allow detection of a previously missed piece of dangerous code. All three of McAfee's GroupShield, Symantec's Mail Security and Trend Micro's ScanMail allow for both manual (or on-demand user initiated) and scheduled scans. It should also be noted that these information store wide scans will also use attachment blocking and content filtering rules when a scan is performed so it is wise to run them after a rule is updated. Finally, these information store wide scans can cause a heavily load in terms of disk and processor usage on the email system so they should be scheduled during non-peak hours.

6. Quarantine Functions

Quarantine functions are basic core features found in almost all antivirus programs. If an infected object is found and cannot be scanned or repaired, then it can be placed in a holding area where a system administrator can analyze it and take appropriate action. This is an import feature for an antivirus product designed for Exchange Server because there are many different types of attachments that are sent inside messages that might not be able to be scanned. Some examples of typically quarantines attachments are database files, password protected archives and other encrypted files, and files of unknown type to the scan engine. A system administrator can manually review, delete, forward to recipient or forward to alternate recipient any quarantined items. Advanced rules can be constructed on what to quarantine. All three of McAfee's GroupShield, Symantec's Mail Security and Trend Micro's ScanMail

support quarantine functions.

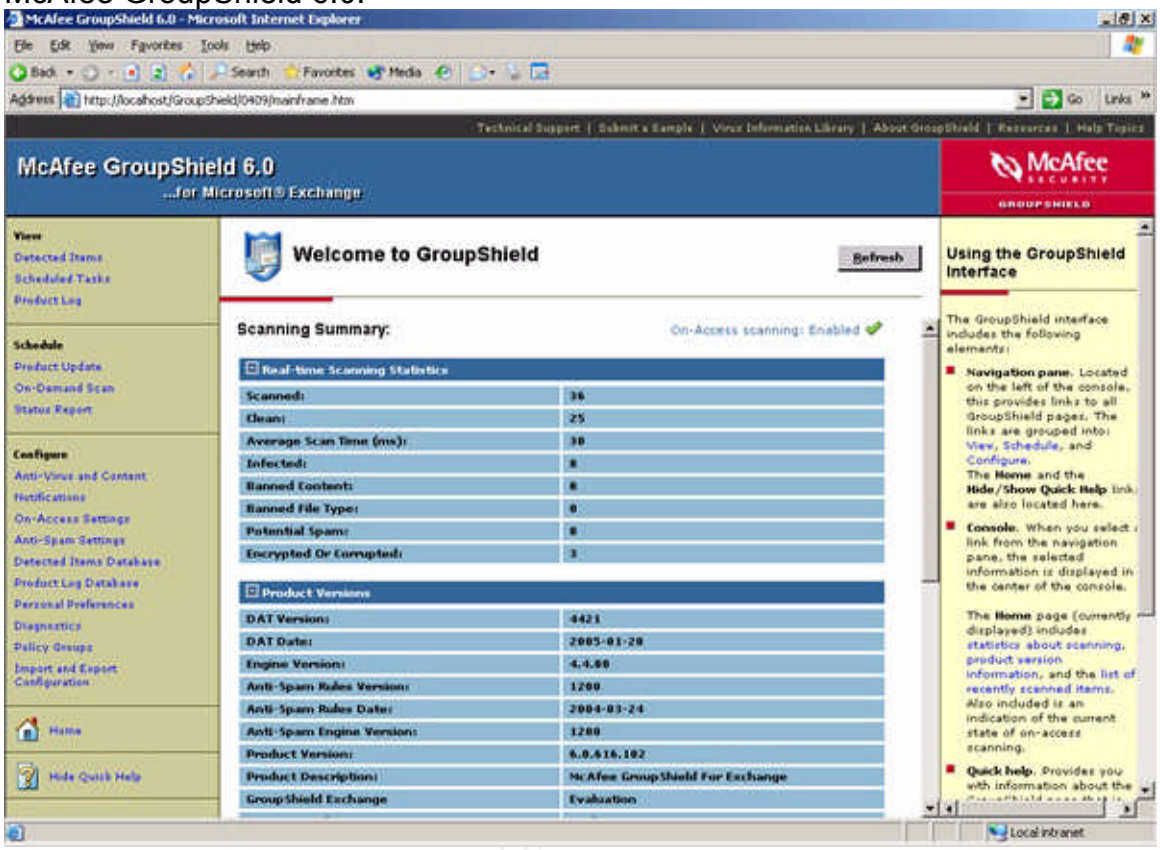
7. Notification Capabilities

An antivirus solution must be able to notify email administrators when there is a problem. Virus detections, quarantine operations and content violations should all produce alerts to inform system maintainers of a detected threat or issue. All three products evaluated could send notification alerts via email, the messenger service, SNMP and to the Windows Eventlog. McAfee GroupShield 6.0 could additionally send notifications to printers and launch external applications. Trend Micro's ScanMail 6.0 has built-in page support for sending alerts.

8. Excellent Management Tools

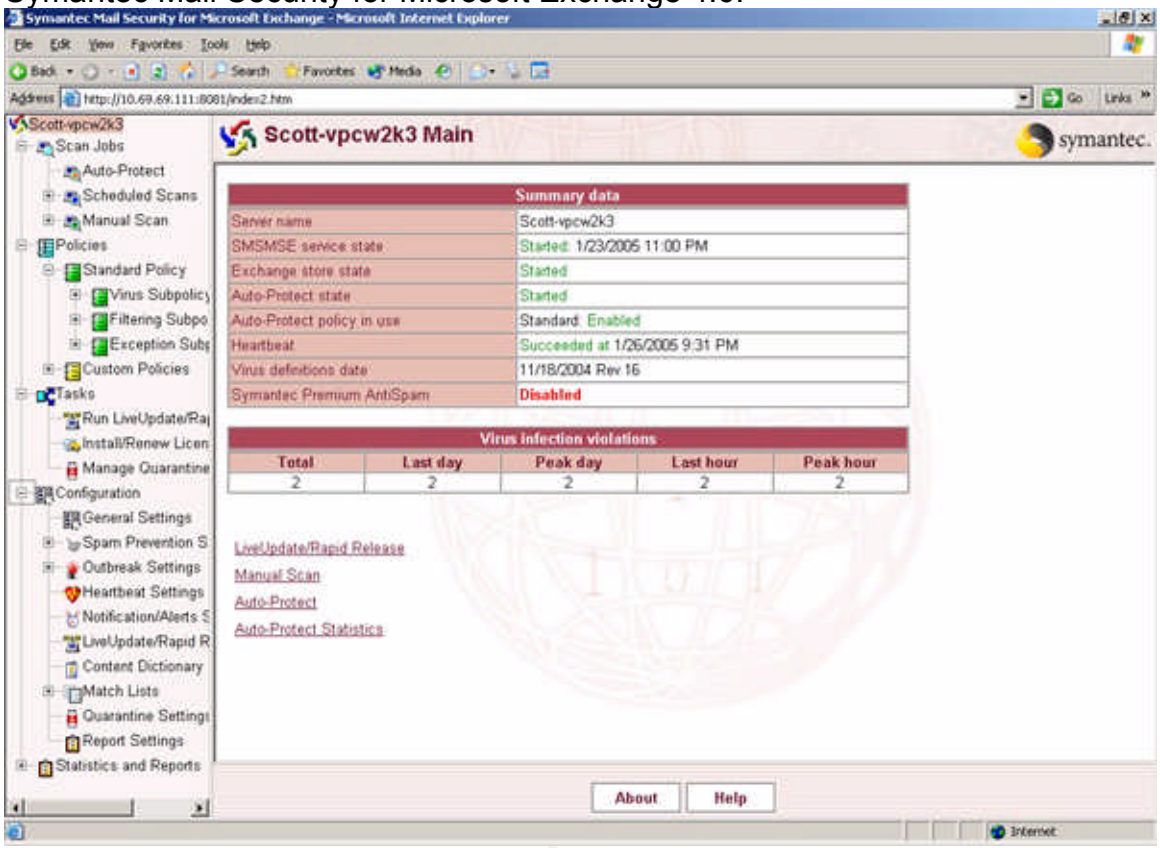
An easy to understand, well designed, intuitive user interface is an important part of any product but especially an Exchange Server antivirus solution. Reporting, administration, updating and policy configuration must all be easy to use and understand through the GUI (graphical user interface). The management interface must be easy enough to use so that issues that need review can be addressed quickly. Both McAfee and Trend Micro's products both utilized the Java virtual machine for portions of their management consoles. From a security standpoint, installing a Java Virtual Machine on the console of any server and especially an email server is not optimal. Fortunately both of products also have web interfaces for management. Symantec's product only offered their management console through a website that is installed to IIS. All three products evaluated had the ability to remotely manage multiple servers from their management consoles. Screen shots of each product are included to display their different implementations.

McAfee GroupShield 6.0:



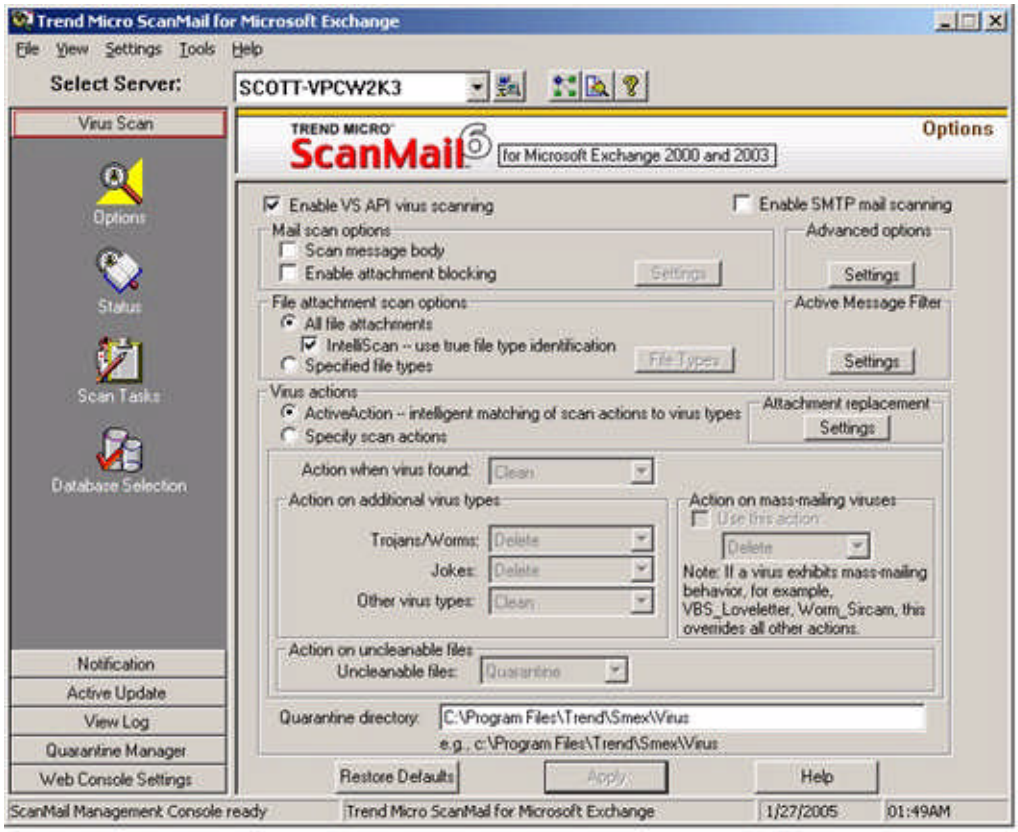
The management console for McAfee's GroupShield 6.0 is reasonably laid out. I did not find the user interface as intuitive as Symantec's or Trend Micro's products. However, I'm sure with enough usage one will become familiar with where things are. This is a screen shot of the website interface which does not require the Java virtual machine and is almost identical to the Java application version.

Symantec Mail Security for Microsoft Exchange 4.6:



The management console for Symantec's Mail Security for Microsoft Exchange 4.6 is very well thought out and easy to follow. The navigation pane provides hierarchal grouping of function along with icons that make sense. The interface is created as a website in the IIS install on the Exchange Server and by default uses port 8081.

Trend Micro ScanMail 6.0:



The management console for Trend Micro's Scanmail 6.0 I found to be the best. It is very well thought out. The navigation pane uses vertical tabs to group like functions along with icons that make sense.

Evaluation Results

All three products evaluated, McAfee GroupShield 6.0 for Microsoft Exchange, Symantec Mail Security for Microsoft Exchange 4.6 and Trend Micro ScanMail 6.2 for Exchange, are mature and capable antivirus solutions. I would recommend any of the three to implement into a production environment. I chose Symantec's Mail Security for Microsoft Exchange 4.6 as the product to write an implementation guide for based mostly on subjective reasons. I found that its mixture of ease of use and excellent functionality made it the best choice for me.

Section 3: Implementation Guide

This section relies heavily on information contained within the Symantec Mail Security for Microsoft Exchange Implementation Guide (for version 4.5). [8] This guide was designed for an implementation on a local single server install of the Symantec Mail Security 4.6 for Microsoft Exchange (to be abbreviated as SMSMSE) on an Exchange 2003 Server.

System Requirements

The system requirements for SMSMSE are very modest and most Exchange Server systems should easily accommodate them. SMSMSE will work with both Windows 2000 Server (or Advanced Server) with Service Pack 4 and Windows 2003 Server (Standard or Enterprise). SMSMSE requires Microsoft Exchange Server 2000 with Service Pack 3 or higher or Microsoft Exchange Server 2003. Enterprise Edition is supported for both versions of Exchange also. The memory requirement is stated as 512 megabytes. Symantec states that required disk space need is 190 megabytes but on the evaluation system installed space used was only about 90 megabytes. Symantec could be overstating the disk space needed for temporary files during the installation process or simply padding for about 100 megabytes reserved space for logs and quarantine. Finally, Microsoft Internet Explorer 6.0 is required to access the management website.

Installation Process

The installation process is extremely straight forward and simple. The following process should be completed on the console of the Exchange Server 2003 with a console user who has administrative rights to the computer. Please note screen shots were only included in this description where they could add value.

1) Run SETUP.EXE
2) InstallShield wizard will begin
3) Press the “Next” button after you’ve read the Symantec welcome screen
4) Press the “Next” button after you’ve read the Setup Preview window with the overview of the installation process
5) Press the “Next” button after you’ve read the Setup Preview window that details the security groups, registry entries and website for the management console that will be created.
6) Press “Yes” button after you’ve read and agreed to the Symantec software license agreement.
7) Press the Ok button after you’ve read the warning message that the temp directory must be excluded from scans if an antivirus file scanner is installed on the server and taken any necessary action if required.
8) Choose if you want IIS to reset after installation (if a previous version of SMSMSE installed choose “Yes”). Press the “Next” button.
If you chose “Yes” for the IIS Reset, a command prompt will appear issuing the command for a few moments.
9) Choose where you want SMSMSE to be installed.
The default location is C:\Program Files\Symantec\SMSMSE\4.6\Server.
Ensure that you have plenty of space for logs and quarantine at the installation location you select.
Press the “Next” button.
10) Select the server name and port number for the management website.

The defaults should be fine unless there is already something on the default port of 8081.

Press the “Next” button.

11) Enter the email address you want to be used for the “FROM” address for notifications.

Press the “Next” button.

12) Select “Yes” or “No” if you are using the Symantec Enterprise Architecture management package.

For my evaluations I did not use this functionality, select “No”.

Press the “Next” button.

13) Review the setup summary

Press the “Next” button.

The setup process will run now for a moment while the installation takes place.

14) Select your Symantec content license file to enable virus definition updates and Premium AntiSpam features if you have one. Your license file must be obtained from Symantec’s Licensing division. You may continue pass this and enter one later, but new virus definitions will not be loaded.

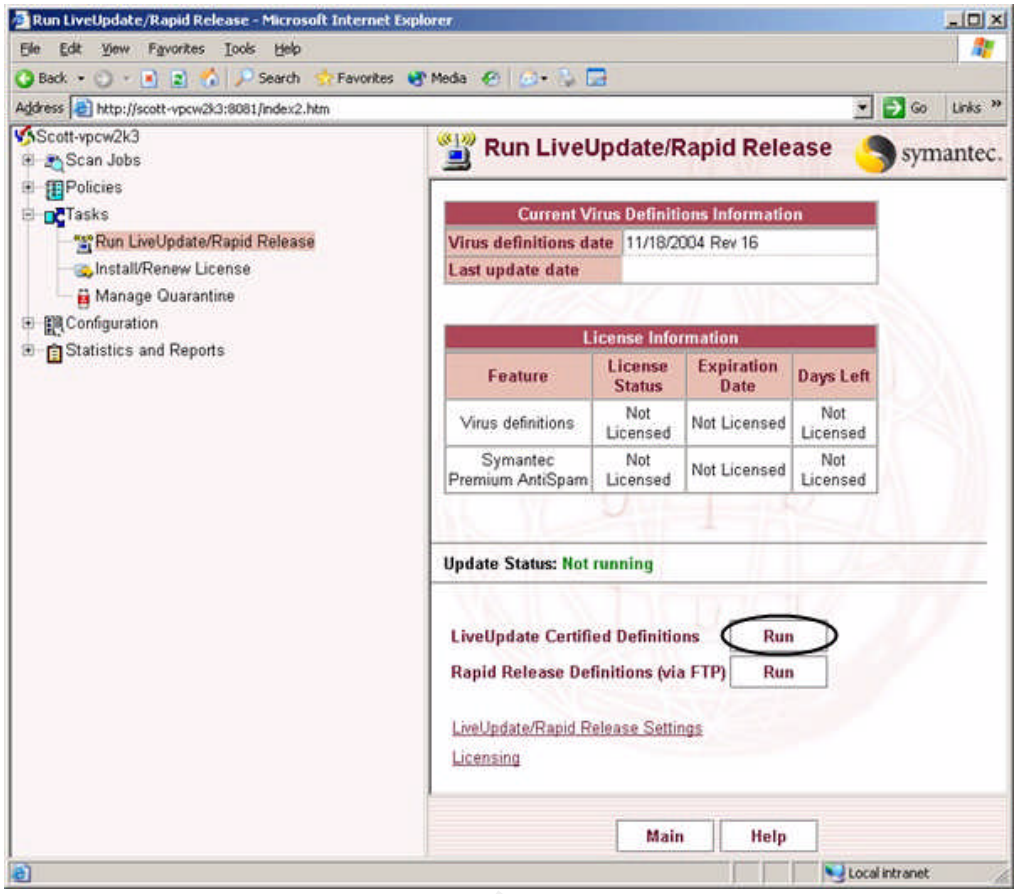
Press the “Next” or “Skip” button.

15) Press the “Finish” button.

The SMSMSE services will start and then the installation is finished.

A desktop icon for the SMSMSE management website is created on the desktop as well as a program group with the management website and a Symantec LiveUpdate icon in it.

16) You should be sure to run LiveUpdate to get the most current antivirus definitions. Open the management console website by clicking the desktop icon and select “Tasks” in the navigation pane. Select Run LiveUpdate/Rapid Release from the navigation pane. Finally click the “Run” button next to “LiveUpdate Certified Definitions.” A screen shot follows to display how to do this:



Configure Process

The default configuration that SMSMSE installs with is very thorough. There are a few settings you should pay special attention to. The following suggested settings work for my environment but may not be optimal for all environments.

The first recommended configuration change is to set LiveUpdate to automatically check for new virus definitions once every 1 hour. There is very little overhead for this operation and the faster you can stop and outbreak the better. In order to make this change, expand “Configuration” in the navigation pane, then select “LiveUpdate/Rapid Release settings.” In the main window, select the radio button for “Run Every” and use the drop down box and select “1” hour.

It’s a good idea to add a nightly scheduled scan job. This change assumes that your information store is not extremely large and that 12:00AM is not a peak production time for the Exchange Server. Take precautions to make sure any scheduled scans do not coincide with any other maintenance jobs like backups or disk defragmentation jobs or server performance could suffer. The user interface is self-explanatory for setting up jobs so the steps to perform this job setup are skipped here.

A configuration change that may not be right for every environment is to modify the built in Encrypted File Rule to quarantine any encrypted file detected

instead of only logging it. A mail administrator may review any encrypted attachment in the quarantine and forward it to the recipient if it's warranted. In order to make this configuration change, expand "Policies", "Standard Policy", "Exception Policy" and select "Encrypted File Rule." In the main window, select "Quarantine attachment/message body, replace with text description" in the drop-down box under the heading "When an encrypted or protected file is detected." Finally press the "Save" button to apply the change.

An essential configuration change is to enable attachment blocking for known dangerous files. SMSMSE comes with a very good match list enumerating most file extensions that may contain threats and rarely included in legitimate messages. To facilitate this change expand "Configuration" and "General Settings" in the navigation pane. In the main window, select "Sample Attachment Name" in the drop-down box under the heading "Attachment Blocking (includes files within containers)." Press the "Save" button to apply the change. The "Sample Attachment Name" match list can be modified by selecting it after expanding "Configuration" and "Match Lists" in the navigation pane.

A critical configuration setting to make sure is correct is for notifications. Expand "Configuration" and select "Notification/Alert Settings" in the navigation pane and set the desired email address in the main window.

The final recommended change is to enable the Hearbeat within SMSMSE. This feature performs a system check of the VAPI threads and SMTP service to insure all services are performing correctly. To enable this function expand "Configuration" and select "Heartbeat Settings" in the navigation pane. Enable and complete the configuration in the main window.

Lockdown Process

The installation of SMSMSE does make a few changes an Exchange Server that an administrator should note.

The installation directory structure should has security applied to it so only administrators and local system have any access. The directory structure for the SMSMSE product is as follows:

..\Symantec\SMSMSE\4.6\Server – program files
..\Symantec\SMSMSE\4.6\Server\AMS – AMS alert files
..\Symantec\SMSMSE\4.6\Server\Downloads - .csv report files
..\Symantec\SMSMSE\4.6\Server\Quarantine – encrypted quarantined files.
..\Symantec\SMSMSE\4.6\Server\Reports – report related data
..\Symantec\SMSMSE\4.6\Server\root – user interface files
..\Symantec\SMSMSE\4.6\Server\temp – temp space for scanning

The services that are installed by SMSMSE are named "Symantec Mail Security for Exchange" and "Symantec Mail Security Spam Statistics." Both services run as local system.

All configurations settings for SMSMSE are stored in the registry under

the key HKEY_LOCAL_MACHINE\Software\Symantec\SMSMSE\4.6. The list of keys and values is extensive and much too long to enumerate here.

The management console website by default is installed to answer on port 8081. It is possible to use SSL to lockdown the management console website so only HTTPS connections are allowed. The process to make this security change is more involved to discuss within this paper but it is clearly laid out in the Symantec Mail Security for Microsoft Exchange Implementation Guide (for version 4.5). [8]

Finally, SMSME creates two security groups, “SMSMSE Admins” and “SMSMSE Viewers”, to control access to the management console website. Once SMSMSE is configured to its desired setup, mail administrators should only use users in the “SMSMSE Viewers” group to for daily usage so as to avoid unintentional changes.

Monitor Process

SMSMSE is a product that will generate notifications whenever an event occurs that requires operator attention. Mail administrators should monitor their email and event logs for notifications of virus, quarantine and heartbeat alerts. Periodic review of the quarantine is a necessity. SMSMSE also collects statistics that should be reviewed dealing with virus, content filtering and spam detection.

Conclusion

It is essential to perform virus scanning of an Exchange Server email system. The threat of malware contained in email messages is real and ever present. All three products which were evaluated offer excellent virus protection and are mature products. As stated earlier, any virus protection solution for Exchange Server should be used in conjunction with other products to form the three tiers or levels of protection so that defense in depth is achieved.

References

1.Weiss, Aaron. “You’ve Got Mail – Messaging Server Trends and Must-Haves” 19 January 2005.
URL: http://www.serverwatch.com/tutorials/article.php/3461461

2. The Radicati Group, Inc. “IBM Lotus & Microsoft – Corporate Messaging Market Analysis” June 2004.
URL:http://download.microsoft.com/download/8/E/8/8E8F3164-D347-4672-A50A-2BCE155FA1E5/IBMLotus.pdf

3. Directions on Microsoft. “Exchange Server 2003, Outlook 2003 Enhance Mobility, Scalability, Security” July 2003.
URL:http://www.directionsonmicrosoft.com/sample/DOMIS/research/2003/07jul/0703i.htm

4. Microsoft Support Webcast Transcription. “The effect of antivirus software on Microsoft Exchange Server” 26 May 2004.
URL:http://support.microsoft.com/?scid=http://support.microsoft.com%2Fservicedesks%2Fwebcasts%2Fen%2Ftranscripts%2Fwct052604.asp

5. Seltzer, Larry. “Who’s Doing Your Anti-virus?” 18 November 2004.
URL: http://www.eweek.com/article2/0,1759,1729254,00.asp

6. Microsoft Press Release. “Microsoft to Acquire Antivirus Technology From GeCAD Software” 10 June 2003.
URL: http://www.microsoft.com/presspass/press/2003/jun03/06-10GeCadPR.asp

7. McAfee. “McAfee GroupShield 6.0 for Microsoft Exchange Installation Guide” November 2003
URL: http://www.mcafeesecurity.com/us/downloads/evals/default.asp
(contained within the GroupShield 6.0 trial

8. Symantec. “Symantec Mail Security for Microsoft Exchange Implementation Guide (for version 4.5)” 2004.
URL:
https://enterprisesecurity.symantec.com/Content/TrialwareForm.cfm?SSL=YES&ProductID=1062&PromoCode=wmailsec (contained in Mail Security trial)

9. Trend Micro. “Trend Micro ScanMail 6 for Microsoft Exchange 2000 and 2003 Getting Started Guide” July 2003.
URL: http://www.trendmicro.com/ftp/documentation/guides/smex62gsg.pdf

Resources

Links to Product Evaluations

Microsoft Exchange 2003 Trial Software
URL: http://www.microsoft.com/exchange/evaluation/trial/2003.asp

McAfee Groupshield 6.0 for Microsoft Exchange
URL:
http://www.mcafeesecurity.com/us/products/mcafee/antivirus/email/gs_exchange2000.htm

Symantec Mail Security for Microsoft Exchange 4.6
URL:
https://enterprisesecurity.symantec.com/Content/TrialwareForm.cfm?SSL=YES&ProductID=1062&PromoCode=wmailsec

Trend Micro ScanMail 6.2 for Exchange
URL: http://www.trendmicro.com/download/trial/trial-us.asp?id=8

Links to Microsoft Exchange Server Resources

Main Microsoft Exchange Server Site
URL: http://www.microsoft.com/exchange/default.mspx

Microsoft Exchange Server TechCenter
URL: http://www.microsoft.com/technet/prodtechnol/exchange/default.mspx\

Exchange Server 2003 Technical Documentation Libary
URL:
http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/default.mspx

Downloads for Exchange Server 2003
URL: http://www.microsoft.com/exchange/downloads/2003/default.mspx

Exchange Server Community
URL: http://www.microsoft.com/exchange/community/default.mspx

Exchange 2003 System Requirements
URL: http://www.microsoft.com/exchange/evaluation/sysreqs/2003.asp

Exchange Server 2003 Solutions Center

URL: http://support.microsoft.com/default.aspx?scid=fh;en-us;exch2003

Microsoft Exchange Server 2003 Deployment Guide
URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=77B6D819-C7B3-42D1-8FBB-FE6339FFA1ED&displaylang=en

Planning an Exchange Server 2003 Messaging System
URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=9FC3260F-787C-4567-BB71-908B8F2B980D&displaylang=en

Exchange Server 2003 Operations Checklists
URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=C5133F35-8E10-4477-B31C-BFD1DC09AB1E&displaylang=en

Exchange Server 2003 Security Hardening Guide
URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=6A80711F-E5C9-4AEF-9A44-504DB09B9065&displaylang=en

What's New in Exchange Server 2003
URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=84236BD9-AC54-4113-B037-C04A96A977FD&displaylang=en

Exchange Server 2003 Design and Architecture
URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=5C76219A-4E30-4B51-A963-4A3896C9BB78&displaylang=en

Exchange Server 2003 Technical Reference Guide
URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=3768246D-C9ED-45D8-BECE-A666143CBA4E&displaylang=en

Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Topology
URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=E64666FC-42B7-48A1-AB85-3C8327D77B70&displaylang=en

Links to other Exchange Server Resources

SlipStick Systems Outlook & Exchange Solutions Center
URL: http://www.slipstick.com/

MSExchange.org
URL: http://www.msexchange.org/