Global Information Assurance Certification Paper

Securing against email viruses in an Enterprise WAN

Rakesh Pitroda
GIAC Security Essentials Certification, Version 1.4b

In year 2000, Company A was attacked by the LOVELETTER virus. The virus was actually introduced into Company A's network by a branch office which was owned by Company Corporate. Consequently, the virus had spread to all the Company Corporate's branch offices and subsidiaries via email. It took over a week to completely eradicate the virus. The loss of productivity experienced by the Company Corporate and its subsidiaries was tremendous. This loss of productivity was unacceptable to the management and a team was assembled to prevent similar disaster in the future.

This case study will describe the steps taken by the Corporate Antivirus Team (CAT) to minimize threats from viruses. As the main objective of CAT was to minimize the threat posed by email embedded virus and other mobile code and not overall corporate security, this paper focuses on the perimeter to end-user/workstation security measures implemented at Company Corporate, its branch offices and its subsidiaries targeted specifically at minimizing risk from email embedded viruses and mobile code.

Before Snapshot

Company A was recently bought by Company Corporate in early 2000. Company Corporate is based in Europe and has many small branches and subsidiaries throughout the European continent and North and South America. Most of these were small independent companies acquired by Company Corporate before the acquisition of Company A in 2000 and as such, most of the branches and subsidiaries had independent LAN.

After the acquisition of Company A, it was decided to converge the small independent LANs into a large WAN to facilitate communications and information sharing. Email being a business critical application for communication, it was a high priority project.

After the WAN links were established, we embarked on the email convergence project. First, a few smaller "business critical" sites in Europe were converged with the headquarters, and then the larger sites were converged. Two of the sites were in North America and the third being the Company Corporate headquarter.

Since all the sites were already using MS Exchange 5.5 server as its email application, the convergence was easy. Most of the work burden of having to rebuild the Exchange server under the Company Corporate's Organization Name and the local Site name was carried by the branch offices and the 2 large sites in North America. Once this was accomplished, the Sites were connected to the Company Corporate's MS Exchange Server using the Site Connector provided with MS Exchange.

At this point in time no security considerations were taken. Except for the Organization Name and Site Name no other restrictions were imposed. Each site

was using its own antivirus product which included Trend Micro, Norton Antivirus and McAfee. The antivirus solutions were implemented at the desk top level. It was not centrally deployed or controlled. There was no regular schedule to update the pattern file; it was done when time permitted. Individual desktop clients had different pattern files. On some desktops the antivirus software was inactive due to lack of appropriate disk space and other desktops had vastly outdated engine and pattern file.

When Company Corporate's network was hit by the LoveLetter virus, it became all too apparent how vulnerable the enterprise network was. Short term security measures were taken by updating the desktop antivirus software engine and pattern files while CAT worked on and implemented an enterprise wide solution.

The CAT consisted of the 3 network administrators from the 3 major sites, 2 in North America and one from headquarters.

During Snapshot

By analyzing what had happened with the attack, CAT realized that to minimize the risk of such an attack a perimeter to end-user antivirus solution was needed. We also realized that the antivirus software alone would not be sufficient; we would also need to educate the users, introduce an email usage policy and develop emergency response procedures.

What happed: LoveLetter is a VBScript worm which spreads through e-mail and has a destructive payload. It overwrites files with specific extensions, modifies registry entries and drops files[i]. It was obvious that an antivirus solution was needed that is able to stop a virus from entering the system; if a virus slips through because the antivirus software was saturated[ii] , the solution should address protection at workstation. The Global Address List (GAL) and the Distribution Lists (DL) needed to be secured to prevent multiple mass mailings. Operating System (OS) needed to be secured so the virus is not able to overwrite files, modify the registry, drop files and download other programs.

Weaknesses Identified:

- Users' propensity to open any email.
- Lack of security on the email server.
- Lack of security on the GAL and DLs.
- Lack of security on the OS.
- Lack of security on the end users' workstation.
- Lack of emergency notification and response procedures.
- Lack of security knowledge of administrators (ourselves).

We started by doing research on our respective antivirus vendors website about viral threats and solutions. Following some of the links provided by them, we quickly became familiar with the wealth of security vulnerabilities information available on the Internet. We found many different articles on different websites. There were articles on OS vulnerabilities, specific application vulnerabilities, intrusion detection, web site hacking, network hacking and countless others.

As our immediate concern was targeted at enterprise wide antivirus solution, we focused our energies on our environment and vulnerabilities. We were using MS Windows NT Server 4.0 SP6 OS on the servers and a mix of Windows 95, 98 and NT on the desktops; MS Internet Explorer versions 4 through 6 for browsers (as there were no controls in place, many users opted to upgrade their browsers whenever and upgrade was released) and Outlook 98.

We first identified different types of known vulnerabilities for this type of scenario. Points of entry were identified as:

- Email
- Web/Internet access
- Floppy/CD ROM drives

Other vulnerabilities were:

- Users
- MS Exchange Server, including GAL and DLs
- OS
- Browser
- Administrators
    - Lack of security knowledge
    - Lack of security response procedures

Email: Email can carry any type of code as an attachment which the user can execute by opening it. Outlook supports the rendering of messages in HTML which can carry embedded malicious code. "Because Outlook, Outlook Express and news readers come linked to IE's HTML rendering Engine, they can also execute scripts."[iii] (Farrow, 68-69).

Web/Internet access: "The term "mobile code" typically refers to interpreted or executable content that can be downloaded and run on a user's workstation."[iv] (Finnegan). Mobile code can be introduced into the network by a malicious website exploiting the web browsers vulnerability.

Floppy/CD ROM drives: End users can introduce infected file or code into the network through the floppy disk or CD.

Users: Users can be the strongest vulnerabilities. "Curiosity infected the network"– users will open anything sent to them just out of curiosity.

MS Exchange: With default installation, MS Exchange is an open application, allowing relaying, no controls for Unsolicited Commercial Email messages (Spam) and even today, no controls for number of messages sent by a single user.

Browser: Internet Explorer is a user friendly browser and has many configurable options, but by default it is fairly open and will execute executable code under the user context

Administrators: Obviously it was our responsibility to secure our systems. In trying to converge our email system, we did not think about the security. We lacked knowledge of the threat so we had no security response procedures in place.

Based on our identified weaknesses and vulnerabilities, we defined our requirements. At this time we were aware that security was a constant work in process; it would not be possible for us to secure all the virus threats at one time.

Requirements

Antivirus

Email servers:
- Scan incoming and outgoing emails
- Automatic pattern update capability
- Frequency of pattern update file
- Ability to scan and block/quarantine/delete attached email files
- Ability to scan ZIP files
- Ability to provide protection for viruses in the wild
- Ability to alert or send notification

Workstations:
- Central deployment capability
- Central Configuration capability
- Push pattern file capability
- Frequency of pattern file updates
- Alert or notification capability

Other Servers:
- Server level protection for file servers
- Gateway level protection for mobile code at web/Internet access
- Frequency of pattern files updates
- Alert or notification capability

After some research, we decided that Trend Micro's solution best met our requirements. Its Interscan Viruswall offered protection for the gateway for HTTP, SMTP and FTP protocols. Scanmail for Microsoft Exchange offered real time scanning of inbound and outbound email, including attachments

utilizing the Antivirus API available with SP4 for Exchange server. Serverprotect offered protection for servers and Officescan Corporate Edition offered real time protection for the workstation with centralized deployment and configuration[v]. Trend Micro's suite was selected not only because it met our requirements, but also we found some good reviews by the users, the pattern file update was not based on subscription, it offered scheduled automatic download and updates of pattern files, program files and scan engine. Though it is more common for major virus vendors to offer these features today, in 2000 it was not so.

Architecture: Our converged email infrastructure used the hub and spoke model[vi] with 2 hub sites. All the other branches and subsidiaries would connect to one of the hub site using Site Connector. In order to join the email infrastructure (create a Site connector with one of the hub sites) the branch or subsidiary (spoke sites) would need to meet the minimum requirements defined by CAT.

MS Exchange Server

OS Configuration: Windows NT 4.0, SP6a. configured as a member server and not as a DC and it should not run any file and/or print services – this was important because if the servers we incapacitated, like we experienced in our attack, it would not affect other network services. The 2 hub sites would be responsible for updating OS requirement with latest service pack and/or hot-fixes. MS Windows NT 4.0 Member Server Configuration Checklist was utilized to secure the operating system, specifically Steps 4 and 5.[vii]

Web Browser: Internet Explorer (IE) 5.5 SP2 with 128 bit Encryption. Although IE 6.0 had been released by this time, it was determined that IE 5.5, SP2 would provide adequate protection against mobile code without introducing new vulnerabilities that were in IE 6.0. The 2 hub sites would be responsible for updating the requirement with latest hot fixes or version upgrade.

MS Exchange: MS Exchange 5.5, SP4. To provide limited defense against DDoS attacks 2 Exchange servers were setup for the 2 hub sites. One server configured as bridgehead server to process all the mail traffic, from and to the internet and through the Site connector[viii]. The 2nd server would host mailboxes and Public Folders. All the other smaller branches and subsidiaries were allowed to have only one server to host the mailboxes, Public Folders and to process all the mail traffic because of financial considerations.

Additionally, default limit of 20MB per mailbox was set at the Private Information Store level. Maximum message size limit of 20MB was set on the

Local MTA level. Maximum message size limit of 10MB was on Internet Mail Service (IMS).

To prevent UCE messages (Spam) restrictions were set on the Routing Tab of IMS to Reroute incoming SMTP mail (required for POP3/IMAP4 support) and appropriate domains added to the list and set to Route to: <inbound>. In the Routing Restrictions… button, on the Routing tab of IMS, Hosts and clients with these IP addresses check box was checked a no entry was added to the list; "… this selection causes the IMS to check for local delivery before letting it upload a message. If the recipient isn't local, the IMS will return 550 Relaying not permitted."[ix] (Neubauer).

All incoming spam messages are collected and the return/reply address is added to the spam list. This list is a simple notepad text file and is used to populate the Turf table registry entry. This accomplishes the same task as adding entries to the Message Filtering option of the Connections tab in IMS properties page. The registry key is located at HKEY_LOCAL_MACHINE on the Exchange server, CurrentControlSet, Services, MSExchangeIMC, Parameters, TurfTable:REG_MULTI_SZ key[x]. Accepted format for the keys are[xi]:

@domain
#domain
user@domain

To protect personal information and prevent possible looping of messages between SMTP servers, out of office replies to the internet and automatic replies to the internet were disabled on the Advanced options, in Internet Mail tab in IMS.

To prevent mass mailings via DL or DL storms restrictions were placed on the DL. Enterprise wide DL and Executive DLs were restricted only to the executive assistants and to HR. Departmental and work group DLs were created and were restricted only the DL members. Exceptions are made to these restrictions pending approval of department supervisor or manager.

Trend Scanmail: Scanmail for Exchange 3.52, Engine.6.5. Real-time Scan should be enabled. AVAPI and MAPI scan methods should be used. All file attachemnts should be scanned and following types should be blocked[xii]:

File Extension	Description/Function of File
.386	Windows Enhanced Mode Driver or Swap File
.ACM	Audio Compression Manager Driver (Windows) and Windows System File
.ASP	Active Server Page

.AVB	Innoculan Anti-Virus Virus Infected File
.AVI	Video, Movie, or Animation Files
.BAT	Batch Processing
.BIN	Binary File
.CLA	Java Class File (usually .CLASS but can be shortened)
.CLASS	Java Class File
.CMD	OS/2, WinNT Command File, DOS CP/M Command File, dBase II Program File
.CNV	MS Word Data Conversion File
.COM	Executable File
.CS*	Corel Script
.DLL	Dynamic Link Library
.DRV	Device Driver
.EML	MS Outlook Express Electronic Mail
.EXE	Executable File
.GMS	Corel Global Macro Storage
.HLP	Windows Help File
.HTA	Hypertext Application (run apps from HTML doc)
.HTM, and .HTML	Hypertext Markup Language (HTML)
.HTT	Hypertext Template
.INF	Information or Setup File
.INI	Initialization file (many)
.JS*, JS or JSE	JavaScript Source Code
.LNK	Linker File, Windows Shortcut File
.MHT*	MS MHTML Document (Archived Web Page)
.MHT*	MS MHTML Document (Archived Web Page)
.MOV	Video, Movie or Animation Files
.MP* and MPG or MPEG	Video, Movie, Animation or Music Files
.MP3	Music Files
.MPD	Mini Port Driver
.MSG	Program Message, OzWin Message/Mail File, MS Mail Message
.NWS*	MS Outlook Express News File
.OCX	Object Linking and Embedding (OLE) Control Extension
.OV*	Program Overlay File (.OVL)
.PIF	Windows Program Information File
.SCR	Screen Saver Script
.SHS	Shell Scrap Object File

.SYS	System Device Driver
.TLB	Remote Automation Truelib Files
.TSP	Windows Telephony Service Provider
.VBE	Visual Basic Script Encrypted
.VBS	Visual Basic Script
.VXD	Virtual Device Driver
.WAV	Sound Files
.WBT	WinBatch Script
.WIZ	Wizard File
.WSH	Windows Script Host Settings File

When a virus is found, the first action should be to clean it, if it is uncleanable then it should be deleted. The infected file should not be backup before any action.

Automatic download of pattern file should be scheduled to occur everyday during off-hours. Automatic update of the scan engine and patch files should not be scheduled because it will be difficult to troubleshoot if any problems arise after the update. Additionally, the problems may not be discovered for an extended period of time since the update is scheduled during off-hours. By updating only the pattern file, we can narrow our troubleshooting to one file.

OfficeScan: OfficeScan 3.54, Engine 6.5. The management console should be installed on a server. Login script should be utilized to check for existing client installations at every login. For every successful logon to the network, the login script should check whether Officescan is installed, if it is not, then the program should be installed and then updated with the latest pattern file; if the program is installed then it should check for the latest pattern file, if it is outdated then the pattern file should be updated. This will ensure that every workstation has the same level of antivirus protection.

The management console should be configured to enable real-time scan of all files, including compressed files. If a virus is found, the first action should be to clean it, if it is uncleanable then it should be deleted. Clients should be allowed to change only the Manual Scan configuration. They should not be allowed to change the Real time scan and other options as it would defeat the purpose of central control and reduce the level of security. No files should be excluded from the scan. Officescan does not allow file exclusion using wild characters, e.g., *.txt, so only specific files can be listed for exclusion.

Viruswall: Version 3.53, Scan Engine 6.1 should be installed at the gateway. All three protocols, SMTP, FTP and HTTP should be enabled. SMTP should be configured for both inbound and outbound traffic. FTP should be configured in the Stand-alone mode. All other configuration options can be accepted at the default level.

Serverprotect: Version 5.3, Engine 6.5 should be installed on all servers. Automatic update should be scheduled daily during off-hours. Real-time scanning should be enabled in both directions, inbound and outbound. All files do not need to be scanned. Scanned file type should list should be the same file extension list that is used for blocking attachments in Scanmail (list provided above). Option to scan floppy, floppy boot area, macrotrap and compressed files should be enabled. If a virus is found, the first action should be to clean the file; if the file is uncleanable, it should be deleted; and infected files should not be backed up before cleaning.

Additional Requirements and Considerations

Although several different options are available from Microsoft to increase security within Outlook 98, we opted to not implement them because we thought it severely limited not only Outlook's functionality, but also how our users use Outlook.

We do require that the users do not utilize the Preview Pane functionality because an email viewed in preview pane can execute mobile code. We also require that users do not utilize the Notification and Open the email function when a new email arrives as this would also execute any malicious code. There is no way to centrally control these settings in our environment, but we feel that with proper user education, we can have good faith that users will honor these requirements.

User Education

Having established and implemented requirements, we educated the users about the necessity of security. We educated the users about the importance of being cautious when opening any files received through email and when surfing the web. We educated them about different types of viruses and malicious code that can be destructive not only to the individual workstation but also to the business unit. Presuming that many, if not most, of the endusers had a computer at home and had internet access, we related the security information to protecting personal information on their computers at home. We felt that by personalizing the information we were providing them, they would adopt "secure thinking" more readily. Guidelines we asked them to observe[xiii]:

- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
- Do not open any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email.
- Do not open any files attached to an email if the subject line is questionable or unexpected (e.g., I Love You, Very Funny, etc.)

- Delete chain emails and junk email. Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
- Do not exercise the option to be removed from spam emails. These emails are sent using unconfirmed email addresses, when you exercise the option to be removed from their email, it actually confirms that your email is valid and in return you will receive more spam.
- Do not download any files from strangers. When in doubt, always err on the side of caution and do not open, download, or execute any files or email attachments. Not executing is the more important of these caveats. If you are in doubt about any potential virus related situation you find yourself in.

We also wrote and published Internet access and Email usage policy. These policies were very broad and stated some obvious provisions about the computer, email and Internet access provided by the company as a tool and service to accomplish their job function/responsibililities. These services should be used with local laws and regulations. These services should not be used abused by using it to gain unauthorized access, impersonation or any other activity that may jeopardize the Company Corporate or its reputation.

Administrators

Lack of Security Knowledge: We gained much knowledge about security during this process and realized the importance of security. It changed the way we administer our network. Through this experience I personally became very interested in the security field and was prompted to pursue this GSEC certification. We subscribe to SANS security newsletter and continue to monitor other security related websites that pertain to our environment. We diligently evaluate published vulnerabilities related to our environment and apply appropriate updates and patches.

Lack of Security Response Procedures: Our Security Response Procedures, as they pertain to virus and mobile code, are rudimentary. When a virus has been identified on the network:

- If it is a single workstation then disconnect the workstation from the network and validate the threat and inform users on the local network to identify if other workstations have been infected by the same virus. If other workstations are infected then stop/disconnect the Site connectors to all other sites and notify the respective administrators; then stop the IMS and inform the local end users with available information about the virus and steps they can take to minimize propagation, e.g., double delete (from Inbox and from Deleted Items folder) the email without opening it. Ensure that each workstation that was reported infected is clean, then notify the users again that they may be receiving more infected emails when we do reestablish the Site

connectors and start the IMS, and the appropriate action they should take to prevent further infections.

- In case of a mobile code from a malicious website, follow the same general principles outlined for a virus infection, substituting appropriate measures to minimize the damage.
- After the cleanup, meet with respective peers to analyze the incident. Identify the vulnerabilities that caused the attack and identify steps to secure the vulnerability. Set a schedule and timeframe to accomplish the task in. Of course, it is quite possible that the vulnerability may be secured during the clean up process itself.

After Snapshot

It was early 2001 when we completed this project Since then we have not experienced any major virus infection incident. There have experienced some isolated incidents when a single workstation or few workstations (fewer than 25) have been infected. Strangely enough these were relatively older viruses and we were able to identify exactly who had introduced them into the network. In these cases, the infection was limited to the Research and Development department where they have more autonomy.

During the Nimda outbreak, users received the email but the attachment had been stripped by Scanmail. We did have a few infections through the web browsing and then through the shared drives, but it was contained and we were able to clean it in a matter of few hours.

Though I have not computed the exact number, by examining the Scanmail logs on a daily basis, we receive approximately twenty to twenty five infected emails a week. All of these emails are identified and removed before they reach the users mailbox. This number does not include the explicit identified attachment types that are removed. These are actual identified viruses.

From time to time we receive emails from our users which they believe maybe a virus. They always make it a point to mention that they have not opened the email, but it looked suspicious. Those emails usually turns out to be a chain letter or spam and a few times it has turned out to be legitimate email, but the subject and the infrequency they receive email from the sender has made them suspicious.

I feel that with that with the solution we implemented, along with some luck, we delivered what our executive committee asked for. Beyond accomplishing the business need, I feel that we, the administrators, have become more aware of the security requirements beyond the virus outbreak prevention and we are working towards addressing security beyond just antivirus solution.

REFERENCES:

[i] Tocheva, Katrin et al., "F-Secure Virus Descriptions." F-Secure. URL: http://www.f-secure.com/v-descs/love.shtml

[ii] Tippett, Peter. " builting "SYNERGISTIC" AV." Information Security. May 2002 (2002): 48-50.

[iii] Farrow, Rik. "The Most Dangerous Software Ever Written." Network Magazine. July 2002 (2002): 68 -69.

[iv] Finnegan, Sean. " Managing Mobile Code with Microsoft Technologies." August 2000. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/mblcode.asp

[v] Trend Micro. URL: http://www.trendmicro.com/en/products/suites/neatsuite-exchange/evaluate/overview.htm

[vi] Paul Robichaux, managing Microsoft Exchange Server, O'Reilly, 1999. 53 -54.

[vii] Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/nt4svrcl.asp

[viii] Posey, Brian M. "Enhancing Microsoft Exchange Server's Security." URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/Exchange55/support/EXCH55KB.asp

[ix] Neubauer, Joseph. " Is your Exchange Server Relay-Secure?" Exchange & Outlook Administrator. January 2000. URL: http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=7696

[x] Toombs, Douglas. "Junk Email". Windows & .NET Magazine. August 1998 (1998). URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=3673&pg=1

[xi] Cochran, Jerry. "The Exchange Server Troubleshooter." Exchange & Outlook Administrator. October 1998. URL: http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=4867

[xii] "Solution 10792." Trend Micro. February 2002. URL: http://kb.trendmicro.com/solutions/solutionDetail.asp?solutionID=10792

[xiii] "Virus Detection and Prevention Tips." McAfee. URL: http://www.mcafee.com/anti-virus/virus_tips.asp