Global Information Assurance Certification Paper

The Shallow Defense – Protecting Email from the Desktop – An Assessment
Daniel Thomaszewicz
GSEC v1.4 Option 2
July 18, 2002

Abstract

Imagine a sheep paddock where the front gate is left open but within the paddock there is a sheep dog to guard each of the sheep. The wolves are on all sides of the paddock. They can come in the front gate. Some of the sheep dogs are young and alert while others are old and tired. The wolves are looking for a weakness. There's no shepherd in sight to raise an alarm.
All you need now is mint jelly to enjoy some fine mutton!
This analogy illustrates the situation in the infrastructure within the business unit I work. Former-management accepted the deployment of a Microsoft Exchange e-mail system without virus protection software, relying instead on desktop-deployed virus protection.

The purpose of my paper is to describe my organization's situation, how we got to that situation and the reasons, our risks, and tools that are in place. To describe what happened to change the early complacency, the actions taken to resolve that emergency, and what was done to prepare for the next one. Also, I hope to suggest means and to convince my leadership that an investment in perimeter virus protection and other steps that can be taken to protect our e-mail and computer infrastructure is a worthwhile and necessary investment.

Background

I perform the day-to-day duties as an e-mail administrator at the headquarters for a wholly owned subsidiary company that is part of a larger corporation. As a service company our business requirements that drive I/T policies are often different then the manufacturing business requirements followed by our parent corporation.
My business unit's business is primarily to provide skilled people to other companies on a contract basis. This means that many of our employees work at customer sites and even at "team member" sites - that is: facilities belonging to other companies. This creates a situation where communications become all-important and from diverse locations that often do not have a direct means of connecting (via "private" network) back to the parent corporation's computer resources.

In the autumn of 1999 it was believed that the e-mail system supporting our facility at that time would fail, as it was not Year 2000 compliant. In October of that year it was determined that our parent company's e-mail system, the use of which was being offered, was not the best choice for our enterprise. Not only was the use of it very costly, but also it could not provide our business unit's

users the support needed in an enterprise such as ours. So it was decided that our business unit should deploy a separate email system, similar to our corporate parent, but different choices would be made to make it cost less and provide more services. And we had to deploy this new system quickly.

Justification for current situation

- Policies: My business unit doesn't often follow the security policies or procedures used by our corporate parent. Some of the reasons are due to the business that we are in. Others are that since our parent company out-sourced I/T there has been much less communication regarding policies from what's left of that I/T group. Additionally, many decisions are made ad-hoc to respond to changing and often unique requirements.

- Access: Due to our employees being in diverse locations we permit POP and Outlook Web Access (via SSL) access to email from the public Internet. Our corporate parent does not.

- Cost: Since the cost of hardware and software (the Exchange software and attended licenses) were a fixed cost, savings were found by not deploying server-side virus protection software.

- Perception: Another issue was the false sense of security from the fact that there had been no (known) successful attacks against our e-mail system that caused data loss.

- Schedules: We all know that I/T projects fall behind schedules. Unexpected issues always arise. Vendors don't produce as expected, technical problems are found, etc. The project to deploy this e-mail system had a December 31st 1999 deadline that was unmovable so a 'basic' e-mail system was to be deployed by that date with no additional (security) software or any other management-type software.

Risks

- The local e-mail servers do not have software that scans incoming or outgoing email or attachments. This means that infected emails are passed on to other e-mail servers and to mailboxes. E-mail clients accessing those mailboxes become vulnerable. Further, the desktops upon which the clients are run become vulnerable. And by extension, other systems within that network become vulnerable. A compromised desktop or e-mail client through an unprotected, unmonitored, e-mail system could spread viruses that did not originate in e-mail.

- We depend on desktops to ensure viruses go no further than e-mail. But this doesn't mean that all desktops using an email client are well

protected. Since we have users that work outside of the facility, it is largely unknown if their desktops receive regular updates. Of course, there's no known product that will stop previously unseen viruses. According to James Michael Stewart's article, several famous viruses infected 70% of the impacted systems within the first 24 hours of their deployment.

- This also means that it becomes almost impossible to determine the extent of possible damage done to other systems, as the virus's "trajectory" is unknown.

- Decentralized virus protection that can be defeated by users who disable the virus protection software, or install software that inadvertently defeats the virus protection software. This may also require more time to update in response to fast-moving, previously unknown viruses.

- Dependency on a single virus detection software vendor can be a risk as software vendors have been known to go out of business, or there is simply a failure to provide an update for a new or unknown virus. Using more than one vendor may mitigate some risk. For example, using server-based virus protection from one company and desktop virus protection from another.

- A virus attack could take down the local e-mail infrastructure. This would impact our entire user base, plus the ability for leadership to communicate with the rest of the business unit and the corporation.

- A virus attack if launched by a compromised desktop could diminish or disrupt services provided by other network servers or infect other desktops.

- End-user satisfaction and trust in the e-mail system and in I/T services in general are downgraded or lost.

- Sending e-mail viruses to our customer's, vendors, or partners email systems would also cause the company potential embarrassment. The customer or partner may simply refuse to receive any additional email from our company for a period of time.

- Another risk is the loss of confidence by customers in our abilities to perform contractual obligations. In our business, the ability to communicate with our customer on a daily basis is crucial.

- It is well documented that virus attacks penetrating e-mail systems cost businesses money. These costs are either in data loss, the loss of employee productivity, or in time spent by I/T staffers to repair and recover

lost or damaged systems. Symantec reports that the Code Red virus cost companies at least $2.5 Billion.

Tools

These were the sole tools used to protect, clean, and react to e-mail borne viruses.

- Network Associates McAfee Virus Scan on the desktop
- Network Associates McAfee NetShield on the servers, which scan the system not the Exchange database or e-mail.
- A CheckPoint Firewall that controls SMTP traffic into the network.

During "Love Letters"

In the spring of 2000 an email virus that was first reported in Hong Kong, but later found to originate within the Philippines, spread over the world impacting government and businesses alike.
The virus became known as "Love Letter" due to the wording (I suspect) of the subject line within the emails in which it was attached. The subjects line was "kindly check the attached LOVELETTER coming from me." If the recipient executed the attachment, the virus using the Windows Scripting Host program, created new system files and modified the system's Windows registry. It also added itself to image files and added the "VBS" extension to those files and replaces other types of files (based on file extension) or modifies the files and 'hides' them.
It also emails passwords lifted from the system to a specified email address and damages the system's boot process.

The day after it became the subject of the nightly T.V. news programs users within our e-mail system began receiving these infected messages from our corporate parent and one of our customer's email systems.
Reaction from our I/T Department was slow at first but soon become three pronged: awareness, containment, and cleanup.
Our Help Desk took care of awareness, informing the user community via e-mail and, where available, telephone broadcasts on what to do (delete the emails with the specific subject line immediately and instructions for how to update their desktop virus software) and informed them of what not to do (launch the virus).
Desktop Support was assigned the task of responding to calls from users who suspected they were infected or given names of users suspected of being infected. The technicians were to disconnect an infected desktop from the network (containment) and remove the virus's traces (cleanup) using instructions provided by the Engineering Team.
The Engineering Team's other responsibility, as e-mail administrators, was to find a way to remove the messages en-mass from within the e-mail servers themselves.

While this was all going on one of our field sites and customers "severed" themselves from our ability to send e-mail to them as they concentrated on their own reactions to the emergency. This action stifled business activity.

Microsoft ExMerge v2

Microsoft provided what the Engineering Team needed for this crisis. A free download of an existing tool, with additional support to aid in removing the infected e-mails from the Exchange database. The instructions provided included program switches which when run searches for, and extracts, e-mail messages with the desired attachments or e-mail subject titles.

I will take the next few paragraphs to describe its installation and use:
You will want to copy the self-extracting download file (from Microsoft's website) onto a system upon which the Exchange 5.5 Administrator Client is installed. I run it on the Exchange server itself.
The download extracts the files to a folder within the system volume named "exmerge" and also creates a subfolder named "exmergedata" that by default is used to store data in Personal Folder (PST) file format archived or copied from the Exchange database.
The executable file, exmerge.exe, comes with one "dll", an "ini" file that can be modified through the tool, a log file, documentation, and two text files; one for "subjects" and another for "attachments".
Microsoft reports that you need to have enough disk space on the volume that contains the Private Information Store (file name is priv.edb) for that file may double in size during the tool's use. I have found this to be true when scanning all mailboxes at once to run the tool (as a requirement, but the tool doesn't really use that much space for all processes), but not when using the command switches I refer to below. You will need enough disk space for the Personal Folder files (PST) that will be created by the tool for each mailbox scanned.
To run ExMerge, the workstation or server must be logged into using an account with Service Account permissions at the Exchange Organization, Site, and Container levels.
You will use either the "attachments.txt" file to search the mailboxes for names of desired attachments or the "subjects.txt" file to search for email that has a desired subject line. I have found that you cannot use both files during the same scan. In one of them you will need to ensure that all lines are "rem-out".
Within these text files you would list the items you wish to scan for and to remove (or copy). I have found that wildcards do not work as asterisks are treated like characters.
If you want to scan the Private Information Store for specific attachments **or** subjects do the following:

1. Log on to the system that has the Exchange Administrator Client using an account that has Service Account permissions and the ability to modify the text and "ini" files.
2. Populate the appropriate text file with the text you wish to scan for.

3. Make sure the other file has no searchable text (using ##~ to comment out the lines).
4. View the "ini" file incase there are specific changes you want to make (i.e.: change the default folder where the resulting PST files will be stored).
5. Run the executable with the following switches:
6. %system%:\exmerge\exmerge.exe –d –b exmerge.ini –srcserv <exchange servername>

-The tool will start running and inform you on progress and upon completion.
The tool doesn't "tell" you if it has found matches for the search parameters. It moves an email that contains a match into a PST file, the name of which is based on the mailbox "directory" name.
The only way to know what you've found is, that I know of, is to open a PST file to view its contents using an Outlook client. In case of a virus search, this is probably not advisable. You'll probably want to delete the PST files right away. One last note, the PST file will have a copy of the mailbox structure (folders) so any file is going to be at least 32K in size.

Fortunately, the "Love Letter" virus caused my facility no loss of data, only lost time and inconvenience. But it did bring home our risks and vulnerabilities.

After "Love"

From the lessons we learned during that event we have instituted the following changes and capabilities:

- The Help Desk has the ability to send advisories to the user community using scripted e-mails to increase the speed of which users become aware of potential or ongoing threats.
- The desktop and server virus software clients are configured to auto update and auto upgrade using a local FTP server where definition and "super-dat" files are maintained after being tested. Users no longer are depended upon to take steps to update their often out-dated virus protection software.
- The Engineering Team has on each Exchange Server the ExMerge tool and the commands needed, and the experience to use the tool to "ferret out" e-mails containing viruses.

But risks remain. The steps outlined in the above paragraph are in most cases reactive, not proactive. It assumes that the Exchange Servers themselves are somehow immune to virus attack and only individual mailboxes within the Exchange database are vulnerable. It also assumes that an e-mail administrator will be available to run a four-hour ExMerge scan of the mailbox contents, during which time virus-infected e-mail could be re-received by the "just swept" mailbox. And, it assumes that a virus outbreak will occur during hours covered by I/T (Help Desk) support.

From my SANS course I have been introduced to the concept of "Defense in Depth", which has made me taken a new look at the steps we had thus far taken. And do we have a long way to go!

Defense in Depth

The title of this paper is "Shallow Defense" because what we are currently doing is the opposite of the concept of Defense in Depth in which multiple layers of defense are used to secure an asset or assets. Applying this to e-mail means at the very least that some kind of virus protection should be placed at the e-mail server and at the desktop client.

And other steps as well should be taken, or at least considered. James Michael Stewart, in his article "Exposing the myth of antivirus", says that relying on anti-virus software is not adequate and he suggests the following steps:

- File attachment filtering before the e-mail reaches the (internal) mailbox
- Communicate and enforce a policy the prohibits the non-business use of e-mail
- Communicate and enforce a policy to prohibit the download or installation of untested software.
- Communicating with users on how to handle attachments
- Within the e-mail client, disabling the execution of scripts

Considerations for Additional Protection

According to a Trend Micro white paper, there are four questions that need to be asked when selecting server-based virus protection software: stability, availability, performance, and scalability.

For this presentation I will look at a product currently used by our parent corporation to provide virus protection to Exchange servers.

ScanMail for Exchange
This would be installed on each of the Exchange v5.5 servers within our organization (there is a separate product for Exchange 2000 for when we upgrade to that application).

Here are the minimum requirements provided on Trend Micro's website:

- 200MHz Intel Pentium or higher
- 128MB RAM
- 50MB free disk space for the program files
- Microsoft Exchange Server version 4.0, 5.0, or 5.5
- Microsoft Exchange Server 5.5 with Service Pack 3
- Windows NT Server 3.51 (Service Pack 5 or higher), NT Server 4.0 (Service Pack 3 or higher), or Windows 2000 Server

- A Java-enabled Web browser that supports frames, such as Netscape Navigator 3.0 (or above) or Microsoft Internet Explorer 3.0 (or above) for Web-based management
- For clustering Windows NT 4 Enterprise Edition and Microsoft Exchange 5.5 Enterprise Edition are required.

Features

- ScanMail scans inbound and outbound e-mail and any attachments for viruses. It can also be configured to filter email based on subject matter or block attachment type.
- This product supports remote setup and server clustering.
- An auto update feature to keep up with new viruses ("virus patterns"), also to update the scan engine, patch updates, and they provide an auto update feature for policies.
- If it finds an unknown virus, that e-mail or attachment can be sent to the vendor for research and if possible, a cleaned file will be returned within 24 hours.
- Activity logs are generated to aid in tracking down the sources of viruses.
- Performance monitoring
- Scans new mailboxes automatically
- Scans attachments in many different formats and multiple compression layers (up to 20 deep).
- Can be configured to send standard or customized alert messages. Although not stated, I will assume these messages are sent via email.
- Management: For management of the software, ScanMail provides a web-based or windows client-based management interface. To access the web-based client, a web browser that supports frames is needed.
- Licensing: Licensing is based on the number of mailboxes being serviced.

Trend Micro also produces a product called "VirusWall" that is deployed on an "e-mail gateway" that scans e-mail and attachments coming from, or going to, an external network (i.e.: the Internet). This product is also deployed by our corporate parent and when used in conjunction with ScanMail. In my present environment no system is used solely as a "gateway" so an additional system would need to be deployed for this product.

Network Associates NetShield for Exchange (5.5) is used successfully by one of our field sites for their customer. Like ScanMail it is installed on an Exchange server and scans incoming and outgoing e-mail and attachments, as well as the mailboxes within that system. It has other features similar to ScanMail. An add-on named Outbreak Manager monitors for certain "behaviors" that could signal a virus outbreak.

On the surface it appears that anyone of these products, combined with processes and procedures for monitoring and quantifying effectiveness, would enhance our present state of security. They would expand our ability to protect

our local network, to add to the reliability of our communications, reduce time spent in break-fix responses, and raise the confidence of our users and our customers in the I/T Department.

Conclusion

E-mail-borne viruses cost companies money and potential business. Developing effective ways to combat the threat also costs money. But the costs of developing an effective defense - policies that direct I/T processes and procedures and end-user actions, deployment of systems to mitigate the risks, configuration of those systems to maximize their effectiveness, monitoring and review of logs to measure effectiveness, and fine-tuning to continually improve – can be far less.
This is a "combat" that is probably not going to end, but likely only to become more prevalent. To borrow a phrase, "eternal vigilance is the price of security".

References

CNN, 'ILOVEYOU' computer bug bites hard, spreads fast, May 2000
http://www.cnn.com/2000/TECH/computing/05/04/iloveyou.01/

McAfee, Virus Profile (for VBS/Loveletter@MM)
URL: http://vil.mcafee.com/dispVirus.asp?virus_k=98617

Microsoft, XADM: Some Questions and Answers About the Exmerge Utility (Q265441)
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q265441

Symantec, 'Security Response', URL
http://securityresponse.symantec.com/avcenter/security/Content/security.articles/defense.in.depth.html

McKenney, Brian, "Defense In Depth", The Edge Newsletter, February 2001,
URL http://www.mitre.org/pubs/edge/february_01/mckenney.htm

INT Media Group, Inc., "malware",
URL: http://www.webopedia.com/TERM/M/malware.html

Microsoft, "Microsoft Exchange Mailbox Merge Program Information (Q174197)
URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q174197

Trend Micro, Trend Micro InterScan ScanMail for Exchange
URL: http://www.trendmicro.com/products/smex/

Trend Micro, InterScan VirusWall - White Paper, November 2000
URL: http://www.trendmicro.com/download/whitepapers/isvw_clusters.pdf

Security.com, Security Tip & Newsletters, Exposing the myth of antivirus, James Michael Stewart, 09 Jul 2002
URL: http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci837177,00.html

Network Associates, (McAfee) Group Shield for Exchange 5.5
URL: http://www.mcafeeb2b.com/products/groupshield-exchange/default.asp

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor