Global Information Assurance Certification Paper

Redundancy on Virus Protection, What?
GSEC Practical Assignment Version 1.2b
Garrett Dietrick, MCSE
April 18th, 2001

Introduction:

Integrity, confidentiality, and availability are the core responsibilities of security in the Infrastructure Technology arena, where they are all threatened by viruses on a daily basis. There is not an all inclusive security solution, enough tools, resources, or training to provide a 100% secure environment. One thing that is true is with a portion of each; there is a greater chance of protecting your organization from attack.

I just spent a weekend out in Dallas, for the K-1 and Security Essentials course. I could not count how many times Eric Cole stated, "Defense in Depth"(1). That is precisely why this paper is being written. There are many companies out there that are placing virus scanners solely on the client machines entrusting that it is adequate enough. Don't get me wrong this is a good thing, but is that enough? The answer is no. There is not a single solution for any corporation's virus security. However, by educating the administrators about solutions and teaching the users about common practices your organization will fend off many attacks.

Policy:

The foundation of any productive virus solution lies behind a well planned out virus policy. One cannot stress the importance of establishing a security policy that provides everyone the opportunity to review and clearly comprehend it. The policy should provide employees information about what their IT staff is providing them and what their IT staff expects from them. Before implementing any new virus solutions, one will need to refer to the existing policy and see how it affects it, and make the necessary changes before implementing the new changes.

Growing problem??

A growing problem we encounter is that viruses are being released daily. Network Associates claim that, "This count (Viruses, variants and trojans) increases by approximately 1000 per month"(2). Is it back and wonder why? Where do people get the time to write these corrupt and harmful programs? Although these questions are intriguing, there is no single answer. The viruses being released these days are well thought out and create a hybrid of threats and vulnerabilities. This issue will never go away, but there are ways for us to protect our organizations to ease this growing problem.

Enterprise Solution
One of the ways to deter this growing problem is to put into place an enterprise solution, one that eliminates some problems at the doorstep of a private network. There are several

ways that a virus can enter an organization, such as messaging, diskette sharing, FTP, web downloading, and hackers. The one area that I am going to focus on is email born viruses, and the varying ways to "Defend in depth" against them. I would like to discuss one particular organization that I had the opportunity to work with and establish a more secure messaging environment.

Prior to the "I LOVE YOU" virus launched on May 4th 2000, this organization's way of combating with viruses was at the desktop level. They relied on having their users update their own virus definitions. Sure there were viruses coming in and infecting machines, sometimes people would be aware of them, and sometimes they would not. Interestingly enough, guess who got hit with the "I LOVE YOU" virus? This virus dropped this 3,500-employee organization to its knees. Approximately 80% of the employee's jobs revolve around email communication, which no longer existed since we were forced to pull the plug. Like many IT professionals, they spent a couple of days on the phone exploring ways to rid themselves of the corrupt program. A couple days later after things were cleaned up, my supervisor called me in and said, "I think that it is time to start researching what we should do about virus protection".

One of the first tools that came to mind was Content Technologies, Mimesweeper for SMTP, now owned by Baltimore. Content Technologies at the time took the stance that "Companies taking advantage of electronic communications consider e-mail as a mission-critical application. But e-mail can also contain hidden dangers leading to network downtime, loss of confidential information and damage to reputation"(3). This product provides a Simple Mail Transport Protocol (SMTP) gateway for messaging. It offers more than just virus scanning, it maintains a rule base for any message that enters it. What happens is the firewall points all of the SMTP traffic to the Mimesweeper server and then that traffic starts a path down a rule base.

Our implementation of the rule base had the message check for a virus first, and then which direction it was coming from, in or going out. We used McAfee's virus scanner, however Mimesweeper is compatible with an array of other vendors. The next step was if a virus contaminated the message, it would be sent to a quarantine folder. Both sender and receiver were then notified that the message contained a virus. A security group in the IT staff would also be notified of the problem.

If the message did not have a virus it went on to the next rule, which asked, is it an executable? If there was an executable attached to the message, then the message was placed in an executable folder. For instance, if the message contained a virus, the program would notify both parties that either they received or sent an executable. In the message that was sent to these parties they were asked if it was work related or not. If it was not work related it would be deleted. Typically, executable files are not work related in a large majority of businesses. There was a bit of hesitation on the organizations part in having executables stopped. They did not realize that a large percentage of these were jokes or harmful programs that were highly likely in containing a virus.

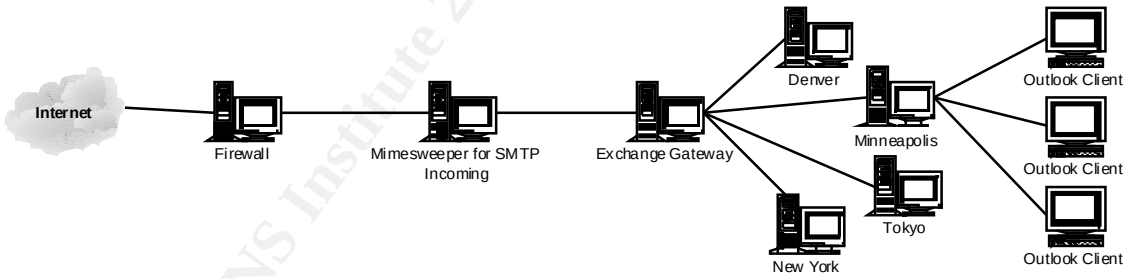
While virus definitions are a good way to protect against existing viruses, one thing that they cannot do is stop groundbreaking viruses. With this in mind we created a rule for messages that contained Visual Basic Scripting (VBS). We monitored any messages that contained VBS and quarantined them, to later evaluate them. Once again, most organizations don't expect to receive many messages that contain VBS.

We then placed a text analyzer after the VBS rule, for words found in viruses that had just come into the wild (out). There were times where it would take Anti-virus companies days to update their definitions for new viruses. So let's say the latest news was there was a virus named Alcatraz. The only step would be to add Alcatraz to the text analyzer, and let it scan the messages for the word.

If a message made it through the rules above, it would then be passed through a scan that determined whether the message was understandable and legitimate. One problem with this method is that if people were using PGP for mail encryption the rule would not know what to do with the message, so it would automatically quarantine it. A possible solution for this problem would be to configure this rule off, since we were doing all the rules above this one only slowed mail down for the users of PGP. That was the only traffic being caught by this rule. This is a limitation of Mimesweeper since there could be virus code located within the encrypted message

The last rule declares that if the message past all the rules above it would be sent the Exchange Gateway, where the gateway would route the message to the appropriate site.

Here is a view of what the process looks like from above:



You say, "Hey that is great, but what if it fails somewhere". Yes, there are areas where the tool can possibly fail and cause problems. Mimesweeper's main role is for perimeter defense. It protects this corporation's outer edge. What if a virus was released from a diskette, say in Denver? It still brings down our network, what should be done?

Server Solution

Part of the resolution is to apply mail server software that also protects against viruses. Right after the "I LOVE YOU" virus hit, Microsoft made available the Anti-Virus Application Programming Interface (AVAPI) for, "Independent software vendors (ISVs) to develop antiviral solutions to scan attachments in the Exchange Server information

Store"(4). Microsoft actually came out with a version of the AVAPI on May 10th 2000, however, it did not work properly (personal experience). Then again on the May 12th 2000, they developed another version, which worked fine. This allowed companies like Network Associate's McAfee GroupShield and Trend Micro's Scan Mail to develop virus scanning directly on the Microsoft's Exchange information store in real-time.

I had the chance to install and work with both GroupShield and Scan Mail and found both providing comparable services. Both of these products provided real time email scanning for viruses. Scan Mail uses a practical user interface that is easy to configure and move around. GroupShield has a snap in into Microsoft's management console (MMC), which is straightforward and configurable anywhere in the enterprise. Both products provide heuristic scanning, which could be an interesting topic to cover in another paper. In general heuristic scanning looks for files that might look or appear to be a virus. It is a nice feature, but provides some false positives.

Trend's Scan Mail was what we decided to go with, but I would also recommend McAfee's GroupShield, they are both good products. One limitation is that these products do not assist at all on an Exchange Bridgehead server. When an organization has many locations and their mail is being sent through a bridgehead server, it would be nice to quarantine a virus to a specific location. There really is not a problem if you install Scan Mail or Groupshield on all Exchange servers, but it would be nice to have a product that scans at the bridgehead server though the Message Transfer Agent (MTA). That way if you had a very large organization spread all over the world one would not have to buy multiple single server licenses, but a single enterprise license that protects at the bridge heads.

Client Protection

Some might say, "Okay we have a SMTP gateway scanner, and also scanners on our servers, how can a virus get through to my machine?" There is always a user that brings in a floppy from home that is contaminated with a virus, which ends up corrupting some major files that everyone in the company uses, now you have an enterprise issue. Or there are users that create internet email accounts e.g. Yahoo, Hotmail, MSN and others that allow you to do email over the internet. This kind of messaging comes through a totally different port than company provided email, which generally is port 25, it comes in on port 80 which is normally setup for Hypertext markup language (HTML). Mimesweeper does not scan this data; neither do Scan Mail or GroupShield servers. The question is what does? Now most of these internet email providers are providing scanning of attachments prior to being downloaded to the client station. Very good thing, but not all mail providers do. The danger occurs when a person opens an email from their browser and it contains a virus. This is an open hole for a virus, but there are ways to protect the client stations as well.

There are many different virus scanners for client machines. ICSA Labs is a division of TruSecure www.icsalabs.com, which is a corporation that provides a list of certified virus scanning software companies and products. The following is a list of some of the

certified ICSA lab certified virus scanning products: "Network Associates VirusScan, Symantec Norton Anti-virus, Sophos, InoculateIT, Kaspersky Anti-Virus, F-Secure, and Trend Micro PC-cillin"(5). These are a few of the products that I would recommend to be installed on client machines. One thing to consider when choosing a virus scanner product is, "What scanners are on the Messaging server or SMTP gateway?" My recommendation is to get something that is different than what you might have on these other levels of protection. The reason here is if a company places all their eggs in one basket or one company, what if the company fails to come up with a virus definition for the next "ILOVEYOU" virus? Remember, Defend in Depth, if there are multiple virus definitions it is more likely catch the virus with one of them, if not both. More is better here. Of course the principal point to make here is that a computer is only protected from the most recent viruses only if they have the most recent virus definitions installed. Either you have the virus scanning application to automatically download the latest definitions, which most of them do, or educate the users how to do it and have them download the new definitions. I generally prefer to have it setup automatically or through a script.

Another issue to acknowledge is updating your messaging client. Many viruses are planned with Microsoft Outlook in mind, since a large percentage of corporations use Outlook as their messaging client. Microsoft has made an effort to help minimize the damage a virus reeks on the client side by providing updates, specifically SR1A, from their website. http://officeupdate.microsoft.com/2000/downloadDetails/Out2ksec.htm. What this specific patch does is "Prevents users from accessing several file types when sent as email attachments"(6). These file types include *.exe's, batch files, com, and other files that might adjust a system. Microsoft also included with this patch a dialog box that pops up when some program that is unknown to Outlook tries to send mail without your knowledge.

Educating your Users:

The final area that really needs to be addressed is educating your users. Many companies will have the greatest virus protection deployed, but if a user does not know what a virus might look like or cause, there are problems. One good way to teach your users about viruses is by having a virus meeting every 6 months or more frequent if it works. You can tell them that there will be free pizza and pop, which catches many people's eyes. Teach your users about viruses and what to look for, and tell them the havoc that they can do. Tell them if they are not sure about something to ask. This is one area that is so easy to do, but is not done enough.

Conclusion

Although you can build a very secure site with tools listed above and educating you users, there are still going to be vulnerabilities. This is why it is so important to create many barriers to hinder viruses entering ones system. Although most of the tools that were mentioned here were from Microsoft messaging, one can apply these principal ideas to other messaging products. The final note is to remember to educate your users;

this is the most important process that a security professional can do to avoid the time and the pain it takes in eradicating that malicious code we call the virus.

References:

Cole, Eric. "Security Essentials." Lone Star SANS
Dallas, 22-26 March 2001.

Network Associates "Virus Alerts." URL:
http://www.mcafeeb2b.com/avert/virus-alerts/avert-risk-assessment.asp (18 April 2001)

Baltimore Technologies plc. "Mailsweeper for SMTP." URL:
http://www.baltimore.com/mimesweeper (18 April 2001)

Microsoft Product Support Services. "Article ID: Q263949; XADM: Understanding How the Antivirus API Scans Attachments."
http://support.microsoft.com/support/kb/articles/Q263/9/49.ASP (18, April 2001)

ICSA Labs "Certified Products, On-Demand/On-Access Anti-Virus Product Certification." URL:
http://www.icsalabs.com/html/communities/antivirus/certification/certprod.shtml (18, April 2001)

Microsoft Corporation "Outlook 2000 SR-1 Update: E-mail Security." URL:
http://officeupdate.microsoft.com/2000/downloadDetails/Out2ksec.htm (18, April 2001)

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event