Global Information Assurance Certification Paper

Shannon Blyth
May 30, 2001
Version 1.2e

Email Quarantine: Take an Extra Step to Protect Yourself

Virus protection is vital to any company in today's world. Because of this, companies must have policies that take the threat of viruses, worms, and other malicious code into consideration when the company makes its electronic security policy. For example, the American Institute of Certified Public accountants and the Canadian Institute of Chartered Accountants uses SysTrust to verify their system's reliability and one of their criteria for security is "There are procedures to protect the system against infection by computer viruses, malicious codes, and unauthorized software."[1] Quarantines for email would be applicable to this point because the main purpose of an email quarantine is to help companies prevent infection of their systems with new viruses that have not yet been added to a virus pattern file.

An email quarantine is a system that is put in place to protect a company from malicious code transported through email. It does this by holding emails that are a potential threat for a period of time so that the company may react in a timely manner by either obtaining the new pattern file for their virus scanners or manually deleting each infected file. By doing so, the email quarantine helps protect against new viruses that may not be recognized by scanners. It is advantageous for any company to use this type of system because it reduces losses due to down time when its computer systems are affected by a virus transferred by email. The major stumbling block with this concept is the lack of products available to deal with email in this manner.

The quarantine would just be one portion of a comprehensive system used by the company to deal with information security. Protection from viruses should begin before the emails have even entered a company's system. This can be achieved by using a product to scan for viruses as they go past the firewall. One such product is TrendMicro's InterScan VirusWall. The main purpose of this product is to delete or clean files at the gateway for viruses that are already known: "Real-time virus detection and clean-up for all SMTP, HTTP, and FTP Internet traffic at the gateway"[2]. This is good to have, but still, it is only a small part of the big picture when it comes to virus protection.

The next step in the virus protection regime of a company would be to use an email scanner on their server. There are many products that fit the bill for this task, such as Norton AntiVirus or TrendMicro ScanMail. There should also be scanners on each workstation to protect from any virus or worm that may slip by, or is brought in inadvertently or on purpose on portable storage media to keep viruses from being distributed elsewhere. Once these methods of virus prevention are in place, the known threats are being dealt with. To deal with the unknown, the quarantine system would be put in between the firewall and the email server scanner so that there has already been an opportunity to check for viruses coming into the system before the quarantine filter is reached. This placement also allows the quarantine to filter all incoming emails before they are sent out to the individual users on the system. If all of these elements are included in a company's virus protection regime, it would be very well protected and should have very few virus problems.

There are many products available to deal with viruses that are already known, but what about new viruses or worms that spread faster than pattern files can be distributed? "The problem is inherent in the design of the Internet, which was initially developed as a means of sharing information in the event of such disasters as a nuclear attack. Simply put, the Net makes it easy for information to spread promiscuously, regardless of where it comes from."[3] This statement sums up the basic reason why new viruses and worms spread so fast. Most virus protection used to deal with email related viruses will check for known viruses, but they aren't able to check for new viruses that are spreading faster than the pattern file can be written. This is where the concept of a quarantine comes in. There are certain types of files that are more prone to transporting viruses or malicious code than others. The company using the quarantine can decide which file signatures are trusted and allow only those to pass through the quarantine. All other file signatures would be put into the quarantine by default for a period of time specified by the administrator of the system, thus giving enough time to get the remedy for the virus before it infects the system.

There are products available that will filter email messages based on content, but they do not have the extra safety measure of holding the emails for a period of time. One or two such as Norton Antivirus 2.0 for Microsoft Exchange do try to take unknown viruses into account, but the vast majority doesn't have a way of dealing with them. The way that Norton Antivirus does this is through the use of a Quarantine server, a centralized server to deal with irreparable, virus infected files. If these products don't meet the requirements of the company considering implementing a quarantine system, they could also consider the option of using a home grown system. This way, the

company can implement it however they want to with features that are specific to the way that the company deals with email messaging.

Using a quarantine, it is more likely that infection of your system by worms such as the Melissa or I Love You virus can be averted. Through use of an in house system to quarantine email, the company at which I am employed was able to stop the Anna Kournikova virus, "[VBS_KALAMAR.A] is a mass mailer that propagates via MS Outlook as an attachment, "ANNAKOURNIKOVA.JPG.VBS"[4], from entering their system before the pattern file was available. The quarantine ran a filter program on the attachments, and, upon finding that it was a vbs file, the email messages were placed in the quarantine queue. Then, through a web interface that listed all of the quarantined emails as well as their attachments, all of the infected emails were deleted.

One of the issues in the design of such a product would be when to release the quarantined emails. How long does it really take between the unleashing of a virus into the wild, and the development of a virus pattern file to deal with it? "In May of 2000, the world shook when a macro virus called 'Loveletter' spread to thousands of e-mail servers world-wide in a mere matter of hours"[5]. The issue is actually about risk management, balancing how long we inconvenience the users due to the possibility of a virus and how long it actually takes for the virus to get around. "Virus protection is a trade-off between security and functionality" [6]. To manage this issue properly, research needs to be done about the type of viruses that are being protected against. On the business side of it, the items that need to be taken into account are how important are the emails that are being quarantined, and how holding these emails will affect the company. What needs to happen after the business is taken into account is that the time an email stays in quarantine must be decided upon by balancing the business risks with the technical risks. When filtering based on the source of the email, if email from a specific source is an absolutely necessity for the business, technical risks may need to be taken to allow that email through the quarantine. On the flip side of things, there may be a high-risk virus and it may be more important to stop the virus than to allow email past the quarantine. If either situation occurs, and they will, the people making the decisions about how long the email stays in quarantine should keep in mind the cost that may result from the virus infecting their systems, and balance that against the cost of business information delivery being delayed.

Another issue would be what type of file signatures should be quarantined. This all depends on what policy the company using the quarantine system has, and what they

deem potentially malicious. What would probably work best is to decide what types are safe enough to allow through and quarantine everything else. One such decision might be to use rich text files rather than more dangerous .doc files. "Use Rich Text Format (RTF) files instead [of .doc files]. All the Word text formatting will be saved, but RTF files cannot contain macros and, hence, cannot be used to spread viruses. "[7] Although this may not be the case anymore, it is an example of something that might be taken into account when deciding which file signatures to allow through. It is also a good idea not to allow emails with executable code in them past the quarantine. "Unfortunately, it is impossible to detect executable code with 100% certainty by analysing either the file content or the file extension. However, blocking files with executable extensions such as EXE, VBS, SHS etc. contributes to overall anti-virus measures."[8] Using a variety of resources, as well as common sense, a good policy declaring what type of files are allowed through the quarantine can be created.

An email quarantine would also be required to deal with mail from different sources in different manners. One instance of such an occurrence would be that internal mail may bypass the quarantine filter even though it contains attachments that are not one of the types allowed through the quarantine. This situation might occur when a company has decided that the business risks involved exceed the technical risks when dealing with email within the company's computer system. That same company might decide that all email coming from the internet should be sent through the quarantine's filter because even though there is business need for some of the email, the technical risks are potentially more dangerous.

Another aspect of quarantine to take into account is how user friendly it is. This factor might be more applicable in the case that a company is using an in-house system but should be considered in any case. There are many ways in which this can be achieved. When using a quarantine to deal with email messages it would be helpful to the user if they could tell what the status of the message is. One way this may be done is to send an email to the recipient when the message is quarantined after being processed in the filter. If they are expecting the email this will let them know why it is taking more time than usual for the email to reach them. As well as the email notification, there might be a tracking system so that the user can just enter an identification number for the email to find out the current status of the email. Another way to increase the user friendliness would be to set up the quarantine so that it does not effect the transfer of internal mail. In theory, internal mail should not be a threat, and, as such, should be treated as though there is no chance of getting a virus from it. Also, there are more likely to be email that has a business value that outweighs the risk of malicious code. The efficiency of the

system is also related to user friendliness and should be taken into consideration. This comment refers to how quickly external mail is processed in the quarantine. The faster the mail is processed, the faster the emails that are not quarantined can get through the system, and the more satisfied the end users are.

Reliability of the quarantine system is essential. If the quarantine process fails, hopefully it will have been designed to fail closed so that nothing will go through the quarantine while it is down. To prevent this from occurring, the process should be run on a highly available, 7 by 24 system. To do this the quarantine process may be placed on redundant machines so that if one fails, the other takes over and mail continues to be processed in the quarantine. If at some point both systems fail, which hopefully they will not happen, the quarantine process should be able to handle processing large amounts of backed up mail. It is necessary that the system have the capability to do this because if the quarantine can't handle it, important mail messages may be lost, or may not be delivered.

In conclusion, use of an email quarantine greatly reduces the risk of a company's computer system catching a virus that has just been released into the wild. It reduces the amount of exposure the company's computer system has to these viruses and worms, thereby reducing the costs to a company due to downtime when a new virus hits. The major issues involved in the quarantine process would be how long to quarantine the email before it is released to the end user, as well as what type of files to quarantine in the first place. Another issue related to email quarantines is the lack of products to deal with email in this manner. Some items to take into account when choosing a quarantine system would be the user friendliness as well as the reliability of the system. An email quarantine would be a good addition to a comprehensive system for the protection of information systems in any company.

[1] SysTrust™ Principles and Criteria, Copyright © 2000 by American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. http://www.aicpa.org/assurance/systrust/princip.htm

[2] TrendMicro InterScan VirusWall. http://www.antivirus.com/products/isvw/ . April 23, 2001.

[3] Chase, Steven. Spam Under Attack. http://rtnews.globetechnology.com/servlet/RTGAMArticleHTMLTemplate/D/20010409/gtspam?tf=RT/fullstory_Tech.html&cf=globetechnology/tech-config-neutral&slug=gtspam&date=20010409&archive=RTGAM&site=Technology . POSTED AT 12:19 AM EDT Monday, April 09 2001.

[4] VBS_KALAMAR.A - Trend Micro Virus Encyclopedia. Trend Micro, Incorporated. http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=VBS_KALAMAR.A April 9, 2001.

[5] Internet Gateway Protection. McAfee. URL: http://www.mcafeeb2b.com/products/internet-gateway-protection.asp. Jan 14 2001.

[6] System to combat e-mail viruses. BBC news. http://news.bbc.co.uk/hi/english/sci/tech/newsid_1294000/1294473.stm. April 24, 2001.

[7] Hruska, Jan. Computer virus prevention: a primer Sophos Plc, Oxford, England. http://www.sophos.com/virusinfo/whitepapers/prevention.html. August 2000.

[8] Hruska, Jan. Computer virus prevention: a primer Sophos Plc, Oxford, England. http://www.sophos.com/virusinfo/whitepapers/prevention.html. August 2000.

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