Global Information Assurance Certification Paper

The Case for a SMTP Gateway Anti-Virus System

LevelOne Security Essentials Practical
Eric Steen
March 9, 2001

The Internet has removed the need for floppies in the spread of computer viruses, and e-mail is now the major means of transport. Originally we had computer viruses that spread via floppy disks. Now we have malware, short for malicious software. Malware is the new generation of network-aware viruses that can replicate and spread like a living organism. An overwhelmingly large proportion of infections today are caused by malware spread through infected e-mail attachments. The ease with which a user can click on an attachment and launch an application is a significant factor in the spread of email-borne malware. The "ICSA Labs 6th Annual Computer Virus Prevalence Survey 2000" illustrates this very well:

> "More than half, 51%, of the respondents had experienced a virus disaster – 25 or more PCs or servers infected at the same time in comparison with 43 % in last year's survey. More than 80% of the respondents had encountered viruses sent via e-mail in their virus disasters. This year our survey shows the remarkable impact of viruses with mass-mail payload or Internet-enabled viruses. In contrast, there were almost no reports of boot sector infectors or infections through diskettes. When comparing these results with those of previous surveys, it is obvious that e-mail is growing in importance as a most important infection vector and diskettes are declining in importance."

The "I LOVE YOU" virus was launched on 4 May 2000. Recipients of this virus thought they had received a "love letter" from an acquaintance. Actually it was a piece of malware that would damage files on the victim's system and then e-mail itself to other addresses in their address book as soon as they opened the attachment. Spreading this way from one machine to another via Internet e-mail attachments, the "I LOVE YOU" virus had infected more than one million computers and caused more than $100 million in damage within a few short hours. In addition, new variants had begun popping up within hours after the initial outbreak.

The magnitude and speed of infection appeared to be a wake-up call for many. Everyone from large corporations down to individual users went on an anti-virus buying spree. PC's were loaded with the latest anti-virus software, and users were warned about the risks with opening attachments. With the latest anti-virus software running on the PCs, users were certain that they were protected, and could not get infected. Unfortunately, it turned out that people really had not learned that much from the "I LOVE YOU" outbreak.

A little less than a year after the "I LOVE YOU" outbreak, on February 12, 2001, a virus that acted in a manner identical to "I LOVE YOU" was released. This time it was packaged as a promise of a picture of Russian tennis player Anna Kournikova. The hacker who released this virus said he wrote the virus not for fun, but in order to prove

that no one learned anything from the outbreak of the "I LOVE YOU" worm a year earlier.

"Clearly, users aren't learning anything from these events," said Graham Cluley, senior researcher at Sophos Plc, an anti-virus vendor based in Abingdon, England. "It's really staggering how many people still open these things."

Users give little thought to security assuming that others are taking care of that for them. Not only are users opening the infected attachments, but also a large number of them have their mail readers set to open the mail in a preview window when it arrives. They will turn off update notices, ignore system administrator warnings, and turn on all the "convenient" options of the software. It appears that the training of users is not working, and steps need to be taken which would remove the user from the equation as much as possible. This is not to say that user training is not important, but there needs to be another layer of protection to fill in the gaps.

Social engineering, the art of manipulating people into actions they would not normally take, is a key factor in the spread of much malware. People depend too much on the software at the PC to catch the malware, and do not pay attention to the e-mail they are opening. If we have learned anything from the "I Love You" and "Anna Kournikova" virus, it is that today's malware can use the Internet and social engineering to spread faster than inoculation and user training. In fact many large enterprises had to completely shut down all mail services, both internal and external, when these outbreaks hit in order to have time to react.

These outbreaks in particular show just how vulnerable a large enterprise with high-speed networks is. Even when anti-virus software has been installed on the PC's it is not always updated often enough, and in some instances you will find that the software is never updated to new virus definitions. The combination of outdated virus definitions and users unaware of the dangers in opening e-mail attachments is a recipe for disaster.

To overcome these problems, we need to employ a layered approach to virus defense, as with any security. Relying on just one layer of virus defense, such as anti-virus software on the desktop, is like a bank with no locks or alarm system. The safe may be impressive, but without the other safeguards it would be relatively simple for thieves to breach the safe undetected, and leave with all the money. Just as a bank needs locks and alarms in front the safe, a network needs anti-virus software in front of the PCs and servers. A firewall will protect a network from hackers trying to come in "the front door", but not necessarily from hackers embedding their code in e-mail and "slipping it through the mail slot".

The Internet gateway, the point that connects the Internet and internal company networks, is a particularly good place to install anti-virus software that will check incoming and outgoing e-mail attachments. What we will be discussing here is enhancing perimeter protection with a SMTP anti-virus gateway. This will be just one layer of the over all

security against malware. Perimeter protection is not meant to replace desktop and server protection, it is just another layer of the over all protection strategy.

Because of the increased use of mass mail payloads for virus distribution, the SMTP anti-virus gateway can provide one of the best overall returns on investment when it comes to protecting corporate assets. Anti-virus software on the gateway can intercept infected attachments before they are delivered to a mailbox. Administrators can update the anti-virus gateway much faster in response to a new virus. It simplifies configuration, and can easily alert system administrators of problems. Multiple email addresses will generate a single virus alert (on the gateway) instead of multiple ones if the infected email is allowed to get through to the desktop.

There are several different ways to implement an SMTP anti-virus gateway. Several firewalls allow for the addition of modules that can scan SMTP mail. Most, if not all, e-mail servers have add-ons available which can perform the scanning of messages prior to delivery. Or you can add a specialized mail relay server, which scans all mail moving in and out of the trusted network.

As with the acquisition of any new technology, due diligence should be exercised in evaluating and selecting an SMTP anti-virus gateway. This includes defining the organization's current posture on e-mail, as well as future needs. No matter which solution you implement there are some basic features you should look for in an SMTP anti-virus gateway product:

- Detects and cleans all known virus and malware
- Provides heuristic scanning
- Provides content filtering
- Ability to scan compressed formats in real-time
- Inability for e-mail to circumvent the system
- Ease of management
- Automated download and installation of updates
- Frequent updates
- Can identify and apply rules to different types of content
- A robust and configurable alert mechanism
- Detailed logging capabilities
- Provides mail relaying protection

The most important aspect of a SMTP anti-virus gateway is that it can detect and clean all known forms of virus and malware. If an infection is found the software should automatically clean or quarantine the infected file. If a message cannot be cleaned, then it should not pass.

The SMTP gateway should employ both a scanning engine to detect known viruses, and a heuristics engine. The heuristic engine applies rules to distinguish viruses from non-viruses and help identify virus variants. Unsophisticated programmers using "virus toolkits" create many of the viruses being released today. These toolkits allow for

variants to be created and released much faster than antiviral software vendors, and system administrators, can update the anti-virus software. To overcome this problem it should be possible for the anti-virus scanning engine to use what it knows about defined viruses to detect undefined viruses.

Social engineering can pose a serious threat to the e-mail system. Ill-informed users can impede the performances of a mail system by spreading a hoax message almost as quickly as a well-written script. Attackers can also trick unsuspecting users into revealing sensitive data by sending an e-mail posing as a system administrator requesting their user ID and password. Because of these threats, you may want to consider a SMTP gateway scanner that provides content filtering. By looking at the text in a message you can stop specific virus hoaxes. It also allows for the creation of rules that can catch many macro virus, and stop sensitive data from be revealed to unauthorized personnel.

Many of the attachments sent via e-mail will be in compressed form. The SMTP gateway scanner should be able to detect and clean infected files even if they are in compressed formats. To be effective, scans of compressed attachments must be performed in real-time. If the scan engine cannot read a file, the SMTP gateway should not let the file pass.

For an SMTP gateway to be effective, it is necessary to put the gateway in front of all incoming SMTP traffic. When deciding where to install a SMTP anti-virus gateway it is important that the system is placed so that all inbound and outbound e-mail traffic is scanned. This means that there is no way around the SMTP gateway, even if the SMTP gateway is down.

If a network has multiple connections to the Internet, it is necessary to put a gateway at each connection, or block e-mail traffic through those connections. If your e-mail policy allows users to use web based e-mail, and/or POP mail, it is also necessary to have a system that can intercept that traffic. If you do not have a system for scanning web based mail or POP mail, your e-mail policy should be changed to forbid this type of mail from the protected network.

The more features an SMTP anti-virus gateway system contains, the more complicated it becomes. The SMTP gateway system should provide a management interface that makes it easy to configure and troubleshoot. Too complex a system can lead to mistakes and oversights in the configuration, leaving the network vulnerable, or causing a disruption in service.

A virus-scanning engine that is out of date is almost as bad as not having virus scanning at all. It should be possible to configure the SMTP gateway to automatically download and install updated virus definitions on a predetermined schedule.

In the second quarter of 2000, the Sophos virus lab was processing 800 new viruses every month. The anti-virus scanner should also include access to frequent and easy to apply software updates, which address viruses that come out in between scheduled updates. The number of new viruses discovered every month continues to increase.

Different types of content represent varying degrees of risk. Encryption keeps virus scans from working, and executable files may represent a risk so great that you ban them completely from e-mail. Because of this, the scanning software should be able to identify different types of content and attachments in messages and apply specific rules to them. The rules should quarantine encrypted messages until anti-virus software on recipients' desktops can be confirmed. As encryption becomes more widespread in the future, it will become even more important to have anti-virus software that can allow or disallow encrypted messages to predetermined groups of recipients. It should also be possible to block messages which contain forbidden file types such as *.vbs.

The scanner should immediately alert system administrators, and the user, upon detection of a virus. The alert options should be adjustable depending on the severity of the issue. Messages with viral code originating from the "outside" are expected, and most likely will need little reaction from system administrators. Infected messages originating from the inside are a completely different matter. An outbound virus signals a breakdown in anti-virus protection on the network and should be treated as an emergency.

As with any good security system, logging is paramount. The SMTP gateway scanner should provide a complete history log, or audit trail, to track the virus' origin. When a virus outbreak is detected, it can be difficult to respond to all alerts immediately. With good logs it is possible to review the path of the virus and ensure that all machines involved have been checked, and that procedures and polices have been modified to keep similar outbreaks from happening again.

A final e-mail threat that needs to be accounted for in an SMTP gateway scanner is mail relaying. Mail relaying is the process of disguising the source of an e-mail by routing it through a duped machine. This technique is commonly used in broadcasting spam. If your SMTP gateway scanner will be configured to send and receive mail directly to the Internet, it will need to provide protection against mail relay. Without this protection your site could end up on a list like the MAPS (Mail Abuse Prevention System LLC) RBL (Realtime Blackhole List) [http://mail-abuse.org/rbl/] causing many sites to refuse your e-mail.

Each network will have different levels of risk and exposure. Dealing with potential threats now, and in the future, requires careful planning. Implementing an SMTP anti-virus gateway, which contains the features discussed here, is just one of the precautions that should be taken in protecting a network against malware.

References:

Birdwell, Lawrence M., Tippett, Peter, "ICSA Labs 6th Annual Computer Virus Prevalence Survey 2000", URL: http://www.trusecure.com/html/tspub/pdf/vps20001.pdf (1 Feb 2001)

Hruska, Jan, "Computer virus prevention: a primer", Sophos Plc, Oxford, England, First published: August 2000, URL: http://www.sophos.com/virusinfo/whitepapers/prevention.html (14 Jan 2001)

Gartner Research, "Virus and Malicious Code Protection: Perspective" 27 June 2000, URL: ftp://ftp.techrepublic.com/cio/prod_analysis/vrscodep.zip (1 Feb 2001)

McAfee, "Internet Gateway Protection", URL: http://www.mcafeeb2b.com/products/internet-gateway-protection.asp (14 Jan 2001)

Buba, Tanya, "Virus prevention checklist", URL: ftp://ftp.techrepublic.com/cio/tools_exe/virusprevention.doc (1 Feb 2001)

Fisher, Dennis, "Anna virus continues to wreak havoc" 13 February 2001, URL: http://www.zdnet.com/eweek/stories/general/0,11011,2685085,00.html (3 March 2001)

Last Updated: July 27th, 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
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 Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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
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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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 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
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS