GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

The Stopgap Measure: Content Filtering
By Dwight F. Daily
Security Essentials Practical

In today's Internet community, when there are new virus' traveling through the E-mail systems, a stop gap measure is needed. While the virus vendors attempt to make the fix, a stopgap measure of a very versatile content scanning tool might just be the solution.

In effectively securing a system there is a need for a multi-layered approach to catching the virus in an e-mail system such as:

TrendMicro's Interscan Virus Wall at the gateway.
Host-based scanner, for the end users machine, such as Norton.
E-mail server scanner such as TrendMicro's Scanmail with content filtering for SPAM.

But where is the stopgap measure to save your system. When that new virus comes out and it is the talk of the Internet, but your vendor doesn't have the solution, how does your company stay secure?

The answer lies in the implementation of a versatile content scanning solution. One such system is Content Technologies MIMESweeper. This type of product has the ability not only to block sender, recipient and subject headers but can also key on particular words and symbol configurations. This flexibility is vital to becoming the stop-gap measure in keeping your system up while waiting for the vendors solution to arrive. The ideal configuration would incorporate all four of these types of products to give a well-rounded sense of protection to your system. Let us look at how each can protect your system and have protected systems when used in conjunction.

Interscan E-mail virus wall has an engine which examines E-mail to determine if the patterns match known viruses or similar to known viruses and attempt to clean the e-mail message and forward. Interscan has the live update option and can have the system update for the manufacture when a new pattern file is ready. This virus scanner has been proven in the past to let virus by its system when they were installed in the body of the message and not in an attachment. In the article by Network Computing, "Trend Interscan Secures Top Virus-Protection Spot," praises for Trend's virus scanning abilities including its ability to clean infected files and sends an undeliverable notification to sender, recipient and Virus administrator when an E-mail containing a virus could not be cleaned (1). Its main purpose should be to delete or clean the known viruses and allow a separate content scanner to do its job. Trend does make a separate plug-in called E-Manager for content filtering. The Interscan Virus Wall has a unique tracking system. Trend's VCS tool "can automatically locate servers on your LAN or WAN that are running Anti-Virus (AV) programs. You can then use Trend VCS to configure the scanning options and upload new virus definition files" (2). There is also a live update configuration to the VCS and notification methods for your anti-virus personnel (2). But be careful how you notify users and the virus team when using a content filter. The

© SANS Institute 2000 - 2005 Author retains full rights.

E-mail generation by the scanning tools can flood the content scanner if the undeliverable message contains the words you are content scanning for i.e. the subject line. Thus creating three E-mail for every virus encountered: one for the sender, recipient, and Virus Administrator (2). It would be wise to turn off notifications once the vendor has a pattern fix in place, just until your system has been cleaned.

The Scanmail is used on the actual mail server prior to the delivery of mail in or out of the system. This is an additional layer that can help contain each domain in a system from the other if there is a virus that does get loose in a particular domain. Scanmail content filtering can block messages based on the header information, disallowing entrance into the system. The virus scanner can block unwanted messages containing virus' by scanning "deep inside attachments to detect viruses buried in multiple levels of encryption and compression" (3). This also helps if the end user has inadvertently introduced a virus into the system via an Internet down load or sneaker net introduction that the host based scanner might not detect. Users love to bring in their newly cut CD that they can load on the system to send picture and the like. These products like scan mail can help catch virus of this ilk not transfer among e-mail domains. Doing regular updates from the vendor is crucial to the success of these systems, but be careful. A colleague informed me of an instance where in the rush to fix a new virus the implementation of a vendor's update crashed a system. The vendor had forgotten a simple line. The customer had not tested it on their mock system and by the time the vendor had corrected the problem, and the information was sent to the appropriate personnel running the servers, a system had crashed and was already being rebuilt. Live updates need to go only to a test system, run on that system, then once your particular system configuration tests OK, install for protection. I was witness to the rebuilding of the system.

The end user host based scanning tool such as Norton's virus scanner can be effective only if implemented. The key is to eliminate the end user from altering the settings for it to scan. Additionally, as noted by the SANS course on desk top Anti-Viral tools care and feeding – live updates should be pushed to the users machines by the administrator and be kept up to date to have the best effect.

With all these in place the extra layer would be a content scanner. The content scanner can scan for: types of attachments, key words (in the body of the e-mail or attachment), favorite subject lines of virus mail, and even block mail intended to steal system information, such as the Win-Bugsfix.exe. Win-Bugsfix.exe was intended to steal "any cached passwords to MAILME@SUPER.NET.PH" (4). When this was known, the content scanner can be used to prevent the sending of such mail. It is apparent that a content scanner is needed as noted by statements from Network computing noting that it took from the time a virus was know in January 1999, "happy99.exe," it took the vendor until its second iteration of a pattern update in February to the virus strain (1). This is possibly the type of situation that Content Technologies International director of marketing, Chris Heslop is talking about when he stated: "Companies relying purely on AV tools for their content security protection have once again been left exposed while

© SANS Institute 2000 - 2005 Author retains full rights.

waiting for the critical fix…[while] MAILsweeper's highly flexible configuration policy editor gives control to the user and allows them to set their security agenda, and not rely on the AV providers" (5).

The key to the whole issue is multi layering of these systems to effectively accomplish the best possible E-mail security for your system. The insertion of the content scanner after e-mail gateway scanners such as Interscan E-mail virus wall and the Server Scanmail is ideal. If you are really conscientious administrator, placing all mail between domains to route from the Virus scanner the content scanner then back to the other systems domain might not be a bad route to take. At least there would be several layers of protections so that one of them might get it but also applying all the same rules then would be applied to E-mail for outside your organization to inside your organization, no one can bypass your security policy except on the local host.

Sources:

(1) PC Magazine Online. "Editors' Choice: NeaTSuite." 6 April 1999 issue of PC Magazine. URL: http://www.zdnet.com/pcmag/features/defendyournetwork/edchoice.html (13 Sept 2000).

(2) Network Computing Editor's Choice. "Trend Interscan secures Top Virus Protection Spot." 5 April 1999. URL: http://www.nwc.com/1007/1007r12.html

(3) Scanmail for Microsoft Exchange. URL: http://conqwest.com/scanmail.htm (12 Sept. 2000).

(4) Maiwald, Eric. "Analysis of the ILOVEYOU worm." GIAC Special Notice. 4 May 2000. URL: http://www.sans.org/y2k/iloveyou_worm.htm (12 Sept. 2000)

(5) Content Technologies/ News Release. "Content Security Company Stops New Virus Threat – 'You've GOT Mail!!!'-At The Gateway." 25 May 2000. URL : http://www.mimesweeper.com/pressroom/news/recent_release.asp?ID=10 (13 Sept 2000).

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.