Security on the Gateways

A white paper by MicroWorld

Abstract

Messaging systems have quickly evolved over the last decade to become an absolutely imperative asset for any organization. But with the increased use of the Internet as a communicational medium, the threat of a virus coming inside an organization has highly increased.

The ICSA, an internationally acknowledged association that keeps tabs on security threats, estimates that 80% of the viruses today enter corporations via the Internet. This percentage is increasing year-after-year & it won't be far when 99% of the threats will come only via the Internet.

The only viable solution is to provide an anti-virus or in a broader sense, security plug-ins, at the gateway level. These plug-ins will very closely work with the email/web server & only provide the security functionality. Since there are many different gateway solutions available in the market, each with a different functionality & a different target market, a single "common" solution on the Gateways is not possible.

Looking at the above trend and keeping in mind the varied functionality, MicroWorld has developed MailScan in a very modular fashion. MailScan is available for almost all of the Mail-Servers available in the market.

Background

With the Internet getting more & more prevalent, more people are communicating through electronic mail than any other medium of communication. In spite of different products & different gateways being used by corporations, electronic communication is possible because of a standard set of rules or protocols followed by all the products and gateways.

According to some estimates, there are over 100 million e-mail users worldwide today. Annual compounded e-mail usage growth exceeds 35%! This simply means that approximately 35 million email users will get added to this communication medium this year. Going by this trend, we should expect to see more than 200 million users worldwide by the year 2001 & you can count on these number growing.

But the downside for the above interconnectivity is the usage of this medium by virus-writers & hackers to create havoc & destabilize this communicational medium. Viruses spreading via e-mail attachments are predicted to become pandemic as more and more e-mail users come into using Internet.

The ICSA, in its 1997 Virus Prevalence Survey, wrote that the current likelihood of an organization encountering a computer virus is on the order of 35 virus encounters per 1,000 PCs per month & the leading method of transmission will be E-Mail.

Types of Virus coming in via the Email medium

Currently, there are over 40,000 computer viruses existing in the computing world. Considering, laboratory viruses, the number might exceed 1,00,000!

In the early years, the only classification of the viruses used to be the Boot-sector viruses and the file-viruses. Boot-Sector viruses used to use the bootable-floppy as its carrier & file-viruses used to use the executable files as its carrier.

When Microsoft released its hugely popular application suites, Word, Excel & PowerPoint, virus-writers specifically started writing viruses using the Macro Language capabilities of these application programs.

Macro Language, as could be gauged, is a very simple way of writing short but complex programs that can be asked to do anything to a computer. Specifically, macro viruses conceal themselves in macro commands in documents and primarily infect Microsoft Word & Excel files.

As you open a document, which has a macro virus, the virus automatically executes & starts showing its contagious nature. The virus can do lots of harm to your data including inserting random sentences in your document and even deleting your important files.

Since documents and spreadsheets are a source of storing information inside files, computer users, using email as the medium, share them. And because documents and spreadsheets flow to-and-fro via the email, macro-viruses too piggyback on these to reach unsuspecting PC users.

This migration of virus distribution from floppy to e-mail attachments tells everything about the evolution of technology. Today plain e-mails without attachments, Java & ActiveX are playing the role of malicious code carriers.

Electronic Messaging – the Evolution:

In the corporate world, the usage of e-mail came up in the late 1960s. Those were the times when IBM & DEC Mainframes used to act like central repository of data and messaging. But, the messaging used was restricted to a Local Area Network or even if a Wide Area Messaging Network was implemented, it was restricted to an organization.

With the Internet boom coming up in the early nineties, proprietary-messaging standards gave way to standard messaging standards. From here came the Simple Mail Transfer Protocol (SMTP), the Request for Comment (RFC822) format, which is still the standard and the Domain Name System (DNS) routing.

Though protocols like the X.400 Message Handling System and the X.500 Directory Services standards are even today used by corporations for internal communications, any inter-corporate communicational system uses the SMTP and the Internet as the medium.

The Internet and SMTP made a great impact on the messaging industry as a whole. With the advent of Personal computers in the 1980s, the LANs blossomed into wide use, even by smaller organizations.

Majority of the e-mail server software's use the SMTP medium for communication purposes.

Viruses posing a strong threat to the corporate network

One singular factor that makes a virus coming via the email as the strongest threat is its ability to replicate fast. Imagine the scenario of how the Melissa Virus spread across the Internet via email: The first user got infected when he opened an infected document. The virus was intelligent enough to scan through the user's Address Book, a file that has a list of e-mail addresses with whom the user regularly communicates, and send itself to all these users.

Assuming that there are 100 addresses in the address book, within a span of about 10-minutes, the virus will reach 100 users. That means, if all the 100-users open this virus attachment, the virus will transmit itself to 100 more users – a total of 10,000 users getting infected! In the next round, 1 million users will get infected!

The exponential nature of the contiguousness is the most disturbing factor of e-mail borne viruses. Within 1-2 days, more than 60% of the world's computers can get infected!

In the above scenario two very important things have got to be taken care of:

- The Internet gateways used for Emails & Web need to be strongly secured using Security Tools. This can be called as the Primary Protection Layer. The Primary Protection layer should be strong and reliable enough to ensure protection at "Port-Level" rather than "purely gateway-level".
- A Secondary Protection Layer need to be used on the Desktops to further minimize any security risks.
- The Security Tools should be intelligent enough to learn and update itself whenever a credible authority publishes a threat.

Having just a Security tool without the intelligence will not be sufficient. Consider the same scenario like the above: In spite of having a security tool on the Gateway, the Melissa can penetrate your network if your security tool is not updated to catch Melissa.

And when Melissa struck large & prestigious corporate networks, who already had a Security Tool installed at their gateways, it only proved that the current range of tools being used, though made for security purposes, are not intelligent.

Server-based Virus Protection provides Manageability & Flexibility:

MicroWorld was the first Security Solutions Company to develop a "real-time" virus-security & content-security solution, specifically designed to work with SMTP/POP3 Servers.

When we say real-time, it means that this is the first solution to be offered on "Port" level rather than "Gateway Level". Port level solutions ensure that TCP/IP Traffic is scanned rather than file scanning. "Port" Level checking ensures that irrespective of the products installed, email checking will compulsorily take place.

MailScan installs on the mail server and transparently detects and cleans viruses hidden in both the Internet Mail and the locally circulating mail before infections can reach the desktop. Because MailScan is server-based, it also has the ability to search mail-databases of old messages to remove existing infections.

Conventional anti-virus products sit at the desktop & react only when the virus has left the messaging system and reached the local hard disk of the PC. Scanning happens only when the user tries to open a mail attachment or save it to the hard drive! This means infected files will be around a network for days before the infection is detected and removed.

MailScan, however, works in real time at the mail server. So e-mails with multiple recipients are scanned only once. Every possible file is scanned; compressed files and zipped files are taken apart & scanned separately. With virus writers now finding ways out to spread viruses without attachments, MailScan also forcibly checks every HTML body.

When a virus is found, MailScan will try to disinfect the virus. If it is able to do this, it re-assembles the clean message & delivers it to the intended recipients. The administrator & the senders are informed of this illegal entry of virus via the e-mail.

High-security environments would prefer to ensure that no executable file enters the organization. MailScan also gives this facility to the

customer. Customers can configure MailScan to delete all executable attachments at the gateway before the email is delivered to the Recipients.

Above all the virus protection is the intelligence of MailScan to update itself automatically. MailScan has a small and tidy web-client inside itself. This web-client continuously communicates with a Server to know whether any new updates or threats have arrived. If so, it automatically downloads the updates and, on a real-time basis, updates the virus-scanner.

Moreover, it also implements a content-control engine within itself. This facility of MailScan can be used to block spam and unsolicited advertising messages sent out by mass mailing companies.

With easy administration features, MailScan makes easy the life of the Systems administrator.

The Future of Gateway Security

MailScan is probably the first security software, with self-learning capability. The greatest boon & the greatest disadvantage of the Internet was always its speed. Information can flow from one end of the universe to the other end within seconds. So, be it a good thing or be it the bad thing, both acts with little delay.

MailScan taps this boon to its advantage using its self-learning capability. It works 24-hours a day & when MicroWorld transmits information saying that a rogue document program is spreading, instantaneously all MailScan security-gateways take this information & update itself.

When MicroWorld transmits information that an email, with a particular subject, is being used by some company to promote itself, this information too is updated by all MailScan's across the world in matter of seconds.

As technology grows faster than any company can update itself, such self-learning techniques are the only ways by which any corporation can keep its security-shield up-to-date.

The future versions of MailScan will do variety of functions like validating an email to put the stamp-of-trust of the sender and knows

which other Gateways of MailScan it can communicate with & accordingly compress the emails with a password for security reasons.