

Protecting Your Organization From Electronic MessageViruses

Robert Grupe 2001-06-04

Protecting Your Organization From Electronic Message Viruses

by *Robert Grupe*, Product Management, *McAfeeB2B Groupware*

last updated June 4, 2001

Introduction

The most important thing to remember about virus protection is that no system is infallible. No matter how good your anti-virus (AV) software is, and how stringent your security processes are, there is still the chance that a completely new virus will enter your organization and disrupt operations. Of course, completely isolating your systems from the Internet and removing them from external e-mail will greatly minimize your exposure; however, in today's digital economy that is no longer a practical option.

The following article is intended to provide you with a checklist of things that can be done to minimize your organization's vulnerability to e-mail borne computer threats.

Protecting The Organization

In order to protect your electronic messaging system, it is necessary to understand the flow of electronic messages within your organization and to provide protection at each point of vulnerability. Prior to the "Melissa" virus, many organizations did not recognize the importance of providing dedicated virus protection for their e-mail systems. The thought was that any virus being carried by an e-mail would simply enter the network as an attachment that could either be detected as it came through the Internet SMTP gateway or by the end-user desktop AV scanner. However, over the past few years, e-mail systems have evolved significantly from simple message distribution to providing collaborative stores, Web-based user interfaces, and access from wireless devices.

The following is a list of basic practices that all organizations should implement as part of their overall security plan.

Establish an organizational anti-virus policy

In order to properly select, configure, and maintain virus protection solutions, your organization

must clearly define what levels of protection and countermeasures it needs. This necessitates specifying the types of data that will be permitted, what content should be filtered or barred, who is responsible for each aspect of the implementation, how communications with end-users will take place, and what actions to take in the event of virus outbreaks and hoax alerts.

Deploy a multi-tiered defense strategy

With the advent of integrated communications technologies, there are now multiple points of entry for infected messages to enter an organization; as a result, it is important to provide virus protection to as many points as possible. This includes the electronic messaging gateways, desktops, PDA's, wireless devices, and the e-mail server itself.

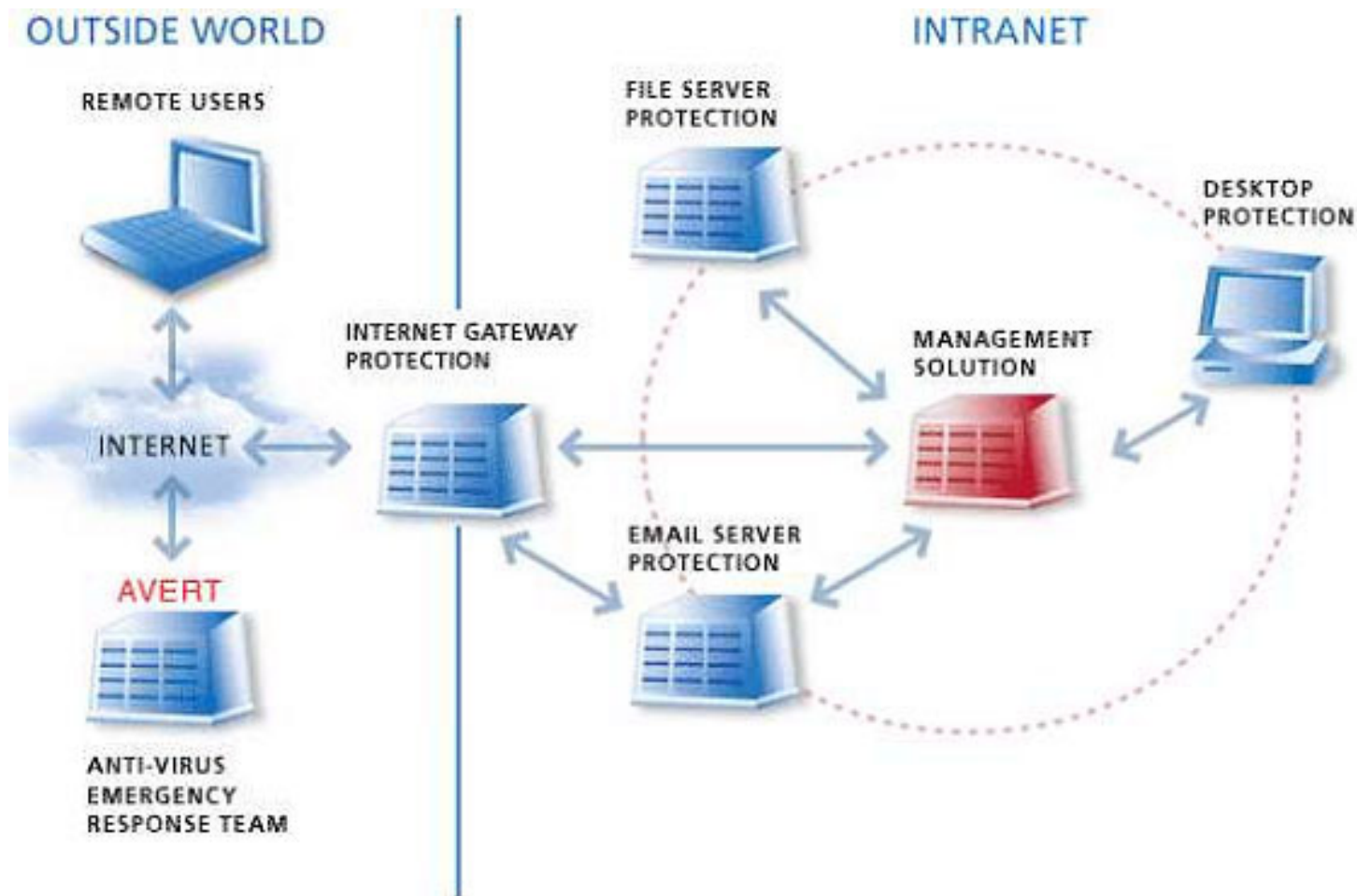


Figure 1: Multi-tiered virus protection system

Update your anti-virus definition files and engines regularly

While most organizations understand the importance of keeping their virus definition files up-to-

date, not everyone understands that it is equally important to ensure that the detection engine is the most current version. Updates can typically be automated, but it is important to periodically check the log files to ensure that the updates are executing properly.

Update your desktop anti-virus software regularly

Server-based e-mail virus protection is the most efficient way to provide protection within an organization, but based upon the particulars of organization's security policy, it is not always able to provide protection for all types of messages (such as encrypted messages). As a result, it is crucial that desktop anti-virus software be updated regularly to provide security that server-based may not be able to offer.

Always keep your operating system, Web browser, e-mail, and application programs up-to-date

Periodically review the security sections of your key software vendors and subscribe to any applicable electronic newsletters to notify you of any new security vulnerabilities and fixes.

Back up your files on a regular basis

If a virus destroys your data, then you can restore them from your archives. E-mail backups and restores can be a bit temperamental, so it is advisable to also have a standard procedure to verify restores from backups periodically.

Subscribe to an e-mail alert service that issues warnings of new virus threats

Many different organizations provide this service, but the most important one will be your anti-virus vendor. The reason is that due to differences in each AV vendor's capabilities, new viruses will be rated differently and the action necessary will vary. For instance, one vendor may have already provided generic virus detection in a past update that provides protection against a new virus and so they would rate a particular virus as a low threat for their customers. However, other vendors who may not be able to provide immediate protection would rate the same virus alert as a "high" risk.

Provide anti-virus overview training to all employees

Most virus outbreaks within organizations could be greatly minimized if the general staff were

aware of e-mail virus vulnerabilities, preventative measures and recommended actions should they encounter a suspected virus.

Protecting E-mail Users

With the closer integration of e-mail and office suite applications, it is no longer sufficient to view anti-virus vulnerabilities solely from the perspective of the e-mail client application. Instead, one must also adequately protect the whole PC that the user is using - whether they are using a local copy of an e-mail application or a remotely-hosted thin client e-mail front-end.

The following is a list of recommended steps that organizations can take to protect end users.

Disable the e-mail program preview pane feature

Some e-mail programs, such as Microsoft Outlook and Microsoft Outlook Express, have a feature that allows users to view a message without opening it in a separate window; however, some viruses can still execute by simply being viewed because the preview pane has the ability to process embedded scripts.

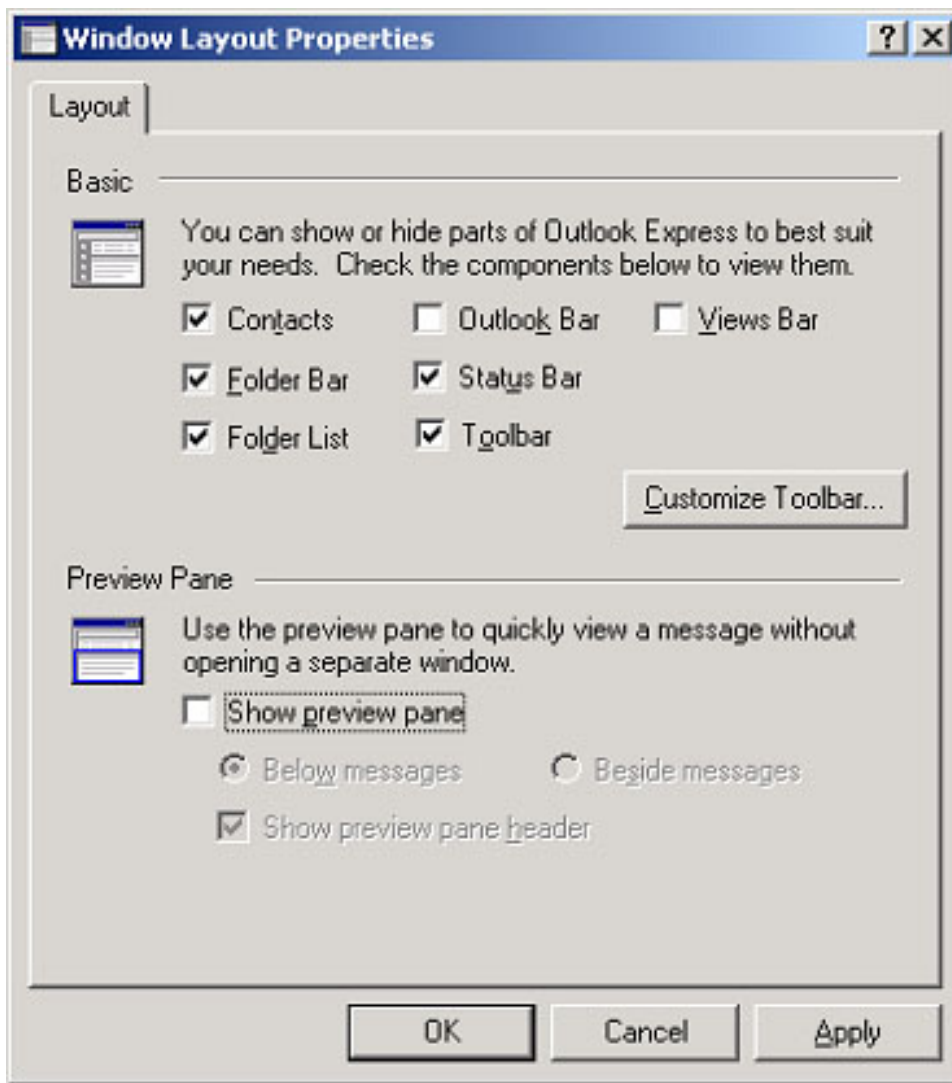


Figure 2: Changing Outlook Express Preview pane settings from the View, Layout menu

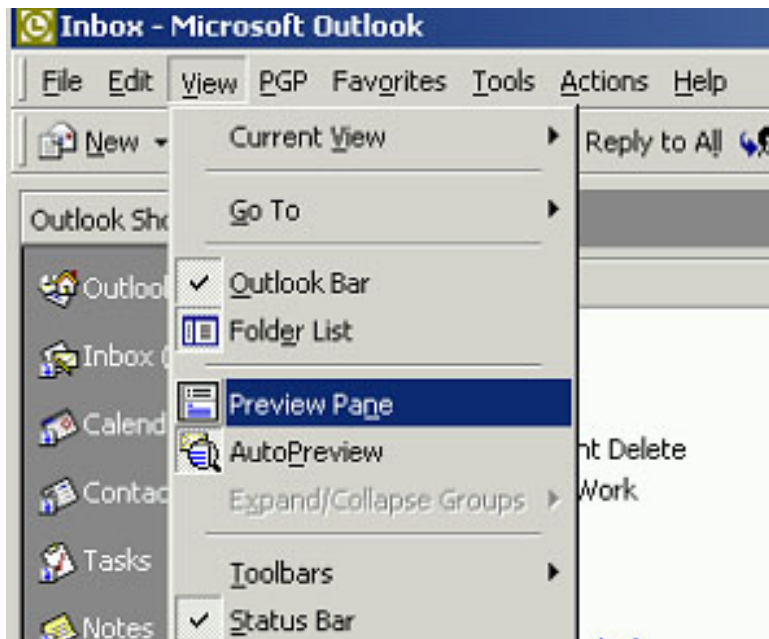


Figure 3: Changing Microsoft Outlook Preview Pane settings

Make the file NORMAL.DOT read-only

If you use Microsoft Word as your e-mail editor, then make NORMAL.DOT read-only at the operating system level. You should also change the Microsoft Word settings to "Prompt to Save Normal Template". Many viruses propagate themselves by changing the NORMAL.DOT file, but this measure can provide at least some deterrent. The permissions can always be switched off again if and when any intentional changes are required.

Use .RTF and .CSV instead of .DOC and .XLS

Use .RTF instead of .DOC formatted word-processing documents and .CSV instead of .XLS formatted spreadsheets because these formats do not support the use of macros. However, even then, caution should be exercised because if the file was first created as a .DOC, it could still contain macros. When exchanging files with others, it is safest to use .RTF and .CSV formatted files, but this should not be relied upon as a fail-safe means of exchanging information.

Remove Windows Scripting Host

If your organization does not use Windows Script Hosting (WSH), then you should consider removing or disabling it. To do this in Windows 9x, go to 'Control Panel' and choose 'Add/Remove Programs'. Click on the 'Windows Setup' tab and double click on 'Accessories'. Scroll down to 'Windows Script Host' and uncheck it and choose 'OK'. It may be necessary to reboot the system. For additional information, visit Microsoft's support Web site.

Use in-box rules to process suspicious e-mails

If your organization does not use e-mail server-based content filtering, then you can use your e-mail inbox rules to automatically delete or move suspect messages into a dedicated folder.

Do not open any files attached to an e-mail from an unknown, suspicious or untrustworthy source

Ensure that the source of any e-mail attachments is a legitimate and reputable one. If you're

uncertain, don't download the file at all or download the file to a floppy and then scan it with your own anti-virus software.

Don't pass along virus warnings from others unless you have verified that it is applicable to your organization

Due to the large number of viruses and hoaxes, unnecessary time and e-mail traffic can be wasted by people forwarding virus warnings that may not be legitimate. Before passing along warnings to others, first check your virus protection vendor's Web site to determine if your systems are already protected or if it is just a hoax.

Write-protect removable media before using them in other computers

If removable media is used to ferry e-mails between computers (such as from work to home), then write-protecting the medium before using it in a suspect system can protect it from becoming infected.

Protecting E-mail Servers

Some organizations believe that as long as they protect their e-mail gateways and internal desktop computers, they do not need e-mail server-based anti-virus solutions. While this may have been true a few years ago, with today's Web-based e-mail access, public folders, and mapped network drive access to the stores, this stance is no longer prudent. Besides viruses entering the e-mail system from the Internet SMTP gateway, infected files can be transferred through an organization's remote Web-based interface, network-connected user devices such as PDAs, disk drives on computers without up-to-date virus protection, or copies from un-scanned archives. Once an infected item gets into the e-mail stores, then only an e-mail server-based solution will be able to detect and remove the infected item.

The following is a list of recommendations that organizations should follow to secure their e-mail servers.

Block common infecting attachments

Many e-mail transported infectors (a.k.a. mass-mailers) use executable files that are commonly found on most computers, such as EXE, VBS, and SHS. Most e-mail users do not need to receive attachments with these file extensions, so these can be blocked as they enter the e-

mail server or gateway.

Schedule complete on-demand scans whenever you update your virus definition files

Even if you keep all of your virus protection up-to-date, it is possible for a new virus to enter your organization before it has been properly identified and a new definition file created for it by your AV vendor. By scanning all of your data with the latest definitions, you can then ensure that there are no undetected infected files in your archives.

Use heuristic scanning

Most of new viruses are simply variants of previously known viruses; however, providing separate detection code for every conceivable variation would be impractical. As an alternative, heuristic scanning looks for known virus characteristics. While this does provide a higher level of protection, it requires more processing time to scan items and may occasionally lead to false-positive identifications. So long as your servers are properly configured, the performance overhead will be worth the additional protection that heuristic scanning can provide.

Use virus outbreak response features in your AV products

Mass-mailer viruses can spread very quickly throughout an organization. They can also be very troublesome for administrators to eradicate while waiting for the appropriate detection driver to be obtained from an AV vendor. Some virus protection products provide features that can configure your system to automatically notify you or take corrective actions if certain virus outbreak characteristics manifest themselves. For instance, you may configure your system to send a cell phone warning if there are more than 50 similar messages received in a short period of time, automatically check the vendor's download site for the latest virus definition files, and then temporarily disable the e-mail gateway until an administrator can respond if the activity continues. This sort of outbreak response policy should be included in the organization's anti-virus policy so that there is a plan of action in place before an outbreak happens.

Archive important data for at least one month

Not all viruses manifest themselves right away; depending upon where a virus is located and how your system is configured, it may take some time for the virus to be discovered. The further back that you can go in your archives, the greater the likelihood that you will be able to

successfully restore an infected item if it cannot automatically be cleaned by your AV solution.

Summary

Over 500 viruses are discovered each month, a trend that is showing no signs of slowing down. As e-mail, business applications, and networked resources become more highly integrated and programmable, the necessity of keeping viruses and malicious code out of your organization becomes increasingly important. Simply scanning e-mails at the Internet gateway no longer provides adequate virus protection. It is hoped that this article has provided some information and insight to help you work with your security vendors to improve the protection within your own organization.

Robert Grupe is a Senior Product Manager in the McAfeeB2B division of Network Associates with responsibility for enterprise electronic messaging and groupware content security solutions. In previous careers, he has been an IT director, online developer and marketing consultant, and other stuff in the aerospace and electro-optic industries.

Relevant Links

[McAfee Virus Glossary](#)

[SecurityFocus Virus Focus Area](#)

[SecurityFocus Virus Mailing List](#)

[AVERT Anti-Virus Tips and Techniques paper](#)

[European Institute for Computer Anti-Virus Research \(EICAR\)](#)

[ICSA Labs](#)

[Microsoft Security](#)

[BugTraq Mailing List](#)

[Virus Bulletin](#)

[Wild List International](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus