Anti-Virus Policy

1.0 Overview

This policy is an internal IT policy which defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

2.0 Purpose

This policy is designed to protect the organizational resources against intrusion by viruses and other malware.

3.0 Anti-Virus Policy

The organization will use a single anti-virus product for anti-virus protection and that product is [redacted]. The following minimum requirements shall remain in force.

1. The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.
2. The anti-virus library definitions shall be updated at least once per day.
3. Anti-virus scans shall be done a minimum of once per week on all user controlled workstations and servers.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

4.0 Email Server Policy

The email server will have additional protection against malware since email with malware must be prevented from entering the network.

4.1 Email Malware Scanning

In addition to having the standard anti-virus program, the email server or proxy server will additionally include [redacted] which will be used to scan all email for viruses and/or malware. This scanner will scan all email as it enters the server and scan all email before it leaves the server. In addition, the scanner may scan all stored email once per week for viruses or malware.

When a virus is found or malware is found, the policy shall be to delete the email and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true. It would simply cause an

additional help desk call by the notified person and most likely waste system administrator's time needlessly. Notifying the recipient that someone tried to send them a virus would only alarm them needlessly and result in an increased number of help desk calls.

Do not depend on your anti-virus software on each computer to prevent these viruses. Viruses have a period of time when they spread unrecognized by anti-virus software. Blocking these file attachments will prevent many trouble calls. Give the users a work around for your network to get some of their files sent to other organizations. Your solution will depend on your network and the software that is being used to block the file attachments. In one case we renamed the file to another type and instructed the recipient to rename it back to the original name before using it. This will not work in all cases since some file blocking software senses the actual file type regardless of its named file extension.

When an email breaks the rules and contains an illegal file attachment your policy should define one of the following to be done:

1. Delete the email and notify neither the sender nor the recipient. The problem with doing this is in the fact that people may be trying to send legitimate files to each other and have no way of knowing their communication attempts are failing. Training by letting users know what files are blocked can help remedy this problem
2. Delete the email and notify the sender - This will notify senders when their emails do not go through, but it will also notify senders who really did not send an email (when a virus spoofed them as the sender) that they sent an email with an illegal attachment. This can cause more additional help desk requests and questions for the administrator on the spoofed sender's side.
3. Delete the email and notify the sender and recipient. - This would have all the drawbacks of the above policy but would also increase help desk calls in your organization.
4. Remove the attachment and let the email go through. - This would let the receiver know that someone tried to send them an illegal attachment. If the attempt was a legitimate one, they could contact the sender and tell them what to do to get the attachment sent. This policy would very likely cause your organization's help desk calls to increase with users calling to ask questions about why someone is trying to send them these files.

There is no ideal policy here and your system administrators must choose the best method depending on the situation being experienced by your organization. I usually use the first option and provide training to users so they know these files are blocked and what the work around is for this situation.

4.2 Proxy or anti-spam Server

To increase mail security, many organizations are adding an anti-spam server or proxy

mail server to their network. This reduces their mail server to the threat of being intruded upon and an anti-spam server can significantly reduce the load on the mail server, not to mention the reduction of spam. Your organization should decide whether to use one of these types of servers or whether to use a service to prevent spam. The service or devices used for this purpose should be defined in this policy. Periodic updates should also be defined and the person who manages the additional servers or is the point of contact for the services should be defined.

5.0 File Exchange Policy

This part of the policy specifies methods that are allowed to be used when files are sent into the network by members of the public or employees of the organization. It specifies:

1. All legitimate methods used including:
    1. FTP transfer to a FTP server.
    2. File transfer to a Web server with a legitimate file upload program.
    3. Any other method.
2. The method and type of software to be used to scan the files for hosile content before they are completely transferred into the network. It will also specify the update frequency for the scanning software.
3. The point in time when the files will be scanned.

6.0 Network Exploit Protection

This part of the policy should specify how hostile software that uses network exploits should be prevented. This policy will not cover system updates but may refer to the system update policy. This policy combined with other quoted policies should prevent worms from entering the network. This policy may also refer to the remote user policy and mobile computer policy.

This policy will specify that all systems be protected by a firewall any time they are connected to the internet. It would specify that systems on the organizational network be connected to a part of the network that is protected from the internet or untrusted network by an approved firewall system. It will also specify or refer to policy that requires computers operating outside the organizational network to have a local firewall software program operational at all times when these computers are connected to the internet. It should specify one or more acceptable software firewall products. This policy may refer to the mobile computer policy which may require users of mobile computers to have their computers checked for malware before connecting to the main network.

7.0Other Malware Policy

This policy should cover any other possible malware including adware and spyware.
It may specify methods to prevent and remove this type of malware. It may specify acceptable prevention and removal software. If the anti-virus product is a product that also handles other types of malware such as adware or spyware, it should be stated here.