SOP:Antivirus Policy

$Author: gozer $ $Id: VirusPolicy.lyx,v 1.3 2002/08/21 09:04:42 gozer Exp $

Viruses are prevalent among the Windows Machine. This document states the policy for detection and post detection of the viruses.

Contents

1 Introduction

Viruses are prevalent among the Windows machines within the network. A policy needs to be published to establish a guideline for prevention and cure of virulent infection on the user machines. This document

provides a set of rules to help system administrators and end users maintain better system uptime of both the servers and desktop computers by keeping the office network free from viruses.

2 Organization

This document will be organized in the following manner:

1. Prevention (Detection and avoidances)
2. Disinfection (Post detection)

3 Prevention

The following guidelines are used for prevention of viruses in the system. Here, we further split the internal system to user machines and the server machines.

3.1 User Machines

- All user machines are mandated to have installed a latest copy of the Norton AntiVirus program.

3.1.1 Virus definitions update

System administrators are responsible for maintaining a repository of the latest Norton Antivirus Virus definition files for the tracking down of the most up to date virus.

A script is used to download a new copy of the latest virus definitions from symantec's website. The script current resides on Bacchus, and will be updated to reflect changes if any on Symantec's Virus Definitions site *Symantec Virus Definition site* `http://www.symantec.com/avcenter/download/pages/US-NNT.html` .

Symantec has packaged their virus updaters in an executable called the SARC Intelligent Updater. The file naming convention used is for every file to have the following:

```
mmddi32.exe
```

(with mm to denote month, dd to denote the date, trailed by the i32.exe)

The file is updated to \\BACCHUS\installers\virusdev\.

3.1.2 Performing the Update

There are 2 types of reminders that are enforced to remind users to update their virus definitions.

- Email notification An email is generated when the virus definitions are downloaded and obtained. The email is sent to the localstaff email alias which should include all staff of eXtropia.

- Domain Logon An update of the antivirus definitions is suggested every time the user logs on to the domain. A logon script on BACCHUS ensures that the users receive the antivirus definitions. The logon script will be covered in the SOP dealing with the Samba share. The logon script should be a DOS formatted file since Windows machines are unable to handle files with only <Carriage Returns> instead of the <Line Feed> <Carriage Return>.

```
NET USE X: \\BACCHUS\Installers
X:
CD \VIRUSDEV
EXPORER <VIRUS DEFINITION FILE>
```

- Every user has a part to play in the virus policy of the company. Users must be responsible and ensure that their systems are running with the latest updated copy of the AntiVirus Definitions.
- Sys team members will conduct spot checks to ensure that the policy of updating the virus definitions is complied with. The spot check should be of a form so that users get the idea that virus in the company is a strict and important aspect of company policy.

3.2 Server Machines

3.2.1 Sophos

Sophos Anti-Virus is a complete anti-virus solution with network functionality at its core. It was designed specifically for the corporate network and offers an easily updated, flexible business solution for managing the complexity of networks from small local area networks to large multi-server, multi-platform WANs.

Sophos is the virus scanning tool used by the virus filtering system, it is easy to install/manage and is updated quite often. It comes with a virus scanning library and a command line tool called sweep. For more information check the sweep man page and the sophos home page *Sophos Home Page* `http://www.sophos.com` .

The download is a manual process that should be done once monthly to obtain the latest copy of the sophos antivirus software. To perform the download, the following provides a simple set of instructions to obtain the latest copy of sophos:

1. Go to *Sophos* `http://www.sophos.com` , and click on the "Download" option on the sidebar.
   (a) On the next page, select to download "Products and Updates".
   (b) On the "Sophos Anti-Virus: Download Products and Updates" page, select that "I would like to evaluate Sophos Software".
   (c) On the next page, select "Home user" and select "Singapore" in the drop down Country list, and click on the "Continue" button.
   (d) The site will then ask for the "Name", "Email", "Phone", "Address" and "Zip Code" of the evaluator. Just key these in and continue.
   (e) On the "Download products and updates" page, select "Sophos AntiVirus for Unix".
   (f) On the page with a listing of the products that are used for Unix operating systems, select the one that says "Linux libc6".

(g) The next page should then have the package with the name "linux.libc6.tar.Z". Download the copy to the local file system, and rename it so that the name has the form sophos-X.XX.tar.gz where X.XX is the version number as given by Sophos.

(h) Untar the file, and it should create an sav-install directory. The file "install.sh" should then be run to install the sophos antivirus in the system.

- A script will be run daily to pull the latest copy of the virus definitions from the sophos antivirus website. The script is obtained by running the "wget http://www.sophos.com/downloads/ide/ides.zip".
- The sys team will be constantly up to date with the latest information about the sophos antivirus program. This can be done by ensuring that the virus definition update script performs the notification to the system team as and when possible.

3.2.2 Sophie

Sophie is a daemon which uses 'libsavi' library from Sophos anti virus vendor (*Sophos Home Page* `http://www.sophos.com`). On startup, Sophie initializes SAPI (Sophos Anti-Virus Interface), loads virus patterns into memory, opens local UNIX domain socket, and waits for someone to connect and instructs it which path to scan. Since the database is loaded in RAM, scanning is very fast. (Note: speed of scanning also depends on SAVI settings and size of the file.) It works on Linux, Solaris (Sparc/x86), HP-UX, and FreeBSD. It was made as a part of 'Virge' project, which is a mail/attachment/virus scanning tool, written in C. Sophie can be found at *Sophie Download Site* `http://www.vanja.com/tools/sophie/` .

Being a daemon service, Sophie provides a substantially faster scanning solution than most other available tools, and this was the reason it was picked to provide e-mail virus protection without creating a too large overhead on the e-mail system.

1. Stopping/Staring sophie Just as most common SysV daemons, sophie can be stopped with:

   ```
   $> /etc/rc.d/init/sophie stop
   ```

   And a log message would be:

   ```
   sophie[1137]: SIGNAL [15] caught - cleaning up and exiting.
   sophie: sophie shutdown succeeded
   ```

   To start sophie:

   ```
   $> /etc/rc.d/init.d/sophie start
   ```

   And a log message would be:

   ```
   sophie[13290]: Initializing    : Sophos IDE version 3.59 (detects 74495 viruses)
   sophie[13290]: Socket path     : /var/run/sophie
   sophie[13290]: Timeout         : 300 seconds
   sophie[13290]: Running as user : mail
   sophie[13290]: Socket group    : mail
   sophie[13290]: Max processes   : 20
   ```

```
sophie[13290]: PID file        : /var/run/sophie.pid
sophie[13290]: Sophie version  : 1.35
sophie[13290]: sophie placed in the background [PID: 13291]
sophie: sophie placed in the background
sophie: sophie startup succeeded
```

2. Check sophie status Checking for the current status of sophie :

   ```
   $> /etc/rc.d/init.d/postfix status
   ```

   If successful, you would see something similar to this:

   ```
   sophie (pid 13233) is running...
   ```

   Otherwise, a stopped sophie would look like this:

   ```
   sophie is stopped
   ```

3. Checking that sophie is functioning properly To test if the sophie daemon is functioning properly, find your favorite virus and run this command

   ```
   $> sophie -f $HOME/virus.exe
   Initializing    : Sophos IDE version 3.59 (detects 74495 viruses)
   Socket path     : /var/run/sophie
   Timeout         : 300 seconds
   Running as user : mail
   Socket group    : mail
   Max processes   : 20
   PID file        : /var/run/sophie.pid
   Sophie version  : 1.35
   Scanning file     : '$HOME/virus.exe'
   Scan result       : '$HOME/virus.exe' infected with virus 'EICAR-AV-Test'
   Sophos cleaned up and terminated
   ```

3.2.3 Postfix server (SMTP Servers)

The servers in the office use postfix as the primary mail server. The configuration of postfix is not covered in this document, but is covered in the mail SOP document. The virus policy for SMTP servers is for all mails going from and to the network needs to be scanned. The tools that enable the scanning of viruses are Virge and Sophie.

The postfix master.cf file should include the following line:

```
filter unix - n n - 10 pipe flags=R user=cyrus argv=/usr/local/bin/virge -f ${sender} -d ${user} -a
```

The other configuration required is for main.cf to have "mailbox_transport = filter". This configuration will cause all mails going to the users' mailboxes to be scanned by virge before ending in the users' mailboxes.

3.2.4 Virge

Virge is mail 'scanner' written in C, which replaces/substitutes procmail for a while, checks the incoming mail, and then sends the mail to the procmail. It will check mail for viruses and/or attachment names. Check the FEATURES/README/NEWS files for more details. Virge requires Sendmail and (optionally) AVPDaemon, Sophie or Trophie (to check attachments for viruses).

Virge is used to process each e-mail, extract attachments and process them thru Sophie for inspection. It operates as a delivery filter, so it doesn't have a daemon component so doesn't require maintenance at all.

The only interesting thing worth mentioning is the location of isolated virus infected e-mails in /var/spool/virge/isolated. Whenever a virus is caught, the original infected e-mail will be left in /var/spool/virge/isolated/recipient/Date/Time/

3.2.5 Samba Server

Samba systems shall be configured to run a daily job where all files in the directories are scanned and cleaned nightly.

Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients. Samba is freely available under the GNU General Public License. Samba is configured in the network to perform file and printer sharing. The samba server serves a wide purpose since users need to share files within the network all the time. The configuration and setup of Samba will be covered in an alternative SOP.

The virus policy requires that all samba servers in the network be installed with a virus scanner and that this virus scanner be run on a nightly basis to ensure that the files shared are free of virus.

4 Disinfection

This section will cover cases where there is either of:

1. An outbreak of virus from outside the office
2. Receipient of virus warnings from the mailing system
3. A suspected outbreak of virus from within of the office
4. A confirmed viral infection

4.1 Outbreak of virus from outside the office

This deals cases where there is an epidemic case of virus infestation in the mailing systems in globally.

There will usually be a news notification of this reported in the news before antivirus companies release their patches.

- Users will be notified to update their virus definitions as soon as possible.

- A general notification will be sent to users to notify them of potential headings or clues of emails that may contain the virus.
- Users are notified not to open attachments from strangers since the attachment may potentially contain a virus.

4.2 Recipient of virus warnings from the mailing system

Users and the sys team are notified of potential viruses when:

- Users outside of the company get infected with viruses, and are attempting to send infected mails to the office network
- Users internal of the company send emails that are detected to be viral by the mail system.

4.2.1 External attempts

External users are categorized as either of known external users, and unknown external users. All mails from either group of users will be ignored. The onus is on the designated recipient of the emails who know the external users to attempt to contact them and assist them in removal of their infection.

For unknown sources, if the unknown source was found to be attempting to send multiple mails simultaneously, the email address in question will be added to the black list of email addresses. Black listed addresses are blocked from sending mails to staff in eXtropia.

4.2.2 Internal attempts

While most of the attempts from internal to the office are false positives, a general guideline is applied to ensure that there is really no such infestation.

Upon receipt of an email notifiying the sender and the sys team that a virus has been detected:

- A virus scan of the drive that the email originated from will be done.
- A scan of the imap folder and files will be done from the imap server.

Should a infected file be detected, the situation will be escalated. The user's machine and his emails will be disinfected as per the situation discussed in the later part of this document.

4.3 Suspected outbreak of virus infection in the office

This covers the case of Section 4.2.2, as well as when the user raises the issue that he/she may have been infected unintentionally through the use of material that has been infected. All measures taken up in Section 4.2.2 will be taken up, and the problem will be escalated upon confirmation of viral infection.

4.4 Confirmed viral infection

This occurs when the antivirus utility used by the user confirms that there is indeed a viral infection on the host that it is running on.

The following steps are taken to disinfect:

- The machine is pulled and unplugged from the network.
- The harddrive (infected drive) is loaded on another Windows based machine to perform scanning of the drives that are suspected to be infected.
- Another harddrive (new drive) is installed in the machine and installation for the plaform of the user's choice is initiated.
- Once the infected drive is verified to be fully scanned and the viruses are quarantined, and installation has been completed, the drive is mounted as a secondary drive on the infected host, and the user is given 2 days grace to transfer the relevant information to the new drive.
- The infected drive will then be formatted and prepared for installation on another machine.

5 Conclusion

The measures stated in this document define the rough strategy for the detection and removal of virus signatures from within the network. This document will be updated to reflect changes and requirements in policy.