Guidelines For An Anti-Virus Policy

Justin S.Kapp, Senior Consultant.
Reaper Technologies

Introduction

The virus threat is real. It is not the world-shattering problem sometimes outlined in the pages of the press; nor is it the non-existent ‘urban myth’ suggested by others. Many ‘in the wild’ viruses cause no damage but a significant number are specifically designed to cause data loss. Like other problems facing IT professionals, the virus threat should be assessed realistically. It is important to identify those areas of the organisation which interface with the outside world; and which is the likely source of a virus infection. The appropriate anti-virus tools should be selected, designed to provide a layered defence of the system (perimeter defences, in-depth protection of laptop PCs, desktop PCs and servers, etc.). It is important to look at the way data is handled within the organisation and to take routine precautions to minimise the risk of infection.

What is a Virus?

A virus is a piece of self-replicating code; in other words, it is software, which is designed to copy itself.

On every disk there is a small program that can be run when the machine is started this is stored in placed called the boot sector on floppy disks and on hard disk this is stored in a place called the partition sector and also on the boot sector. Boot sector viruses infect this boot sector of floppy disks and the partition sector or, in some cases, the boot sector of hard disks, when the

PC is booted from an infected floppy disk. Executable file viruses infect program files, on local drives or network drives. Macro viruses infect the macros within document and spreadsheet files.

In addition to the code necessary for the virus to copy itself, most successful 'in the wild' viruses try to conceal themselves, from users and from anti-virus programs. If a virus quickly draws attention to itself, it is unlikely to spread very far. Some viruses contain a payload; this could be anything from a screen display, or message, or damage to data or program files. However, not all viruses contain a payload.

If the virus does contain a payload, there must be a trigger which causes the virus to deliver its payload. The trigger may be a system date, the number of re-boots, the number of floppy disks infected or something else.

It is worth noting that virus authors, unlike commercial software vendors, do not have to make their software compatible with other programs; they do not have to beta test their software or provide technical support on their products; for this reason, viruses may produce unintended consequences.

Identifying the Threat

You can't manage what you can't measure! In order to implement an effective anti-virus strategy, it is essential to identify the sources of any possible virus infection. You should consider the following.

- Floppy disks and CDs brought into an organisation including shrink-wrapped software from original manufacturers and disks from other organisations (suppliers, marketing agencies, etc.) bring with them the risk of virus infection. The movement of floppy disks and CDs between different sites within an organisation may also help to spread a virus. Boot sector viruses are still common, and viruses have been found on CDs.
- Desktop PCs used at home and laptop PCs are a potential source of virus infection. The use of laptop PCs, in particular, has become commonplace in the last few years. Floppy disks and CDs used in these PCs may not have been checked for viruses. The employee may not be the only person using the PC (spouse, children, friends, etc.). It is important to recognise that these PCs, which are not under the direct

control of an organisation's IT Department, may be more exposed to virus infection than those which are under the direct control of the organisation.

- The use of email within corporate organisations provides an effective way for viruses to spread. It is NOT possible to become infected by a virus simply by reading a text message, in spite of the many virus hoaxes ('Good Times', 'Irina', 'Penpal Greetings', 'Deeyenda', 'AOL4FREE', 'Join the Crew', etc.) which supposedly spread via text messages. However, email attachments are a potential threat. Since the advent of macro viruses, which infect documents and spreadsheets, email has become a very effective mechanism for spreading viruses. If a document or spreadsheet is infected, it can become widespread very quickly by being attached to an email message. This is true even of an email system with no connection to the outside world. If users are able to send and receive emailemail via the Internet, the threat becomes even greater.
- Use of the Internet is a further potential source of infection. If any users within an organisation have direct access to the Internet or any online service they are able to download a vast range of material all potentially infected. Any file downloaded could contain a virus: either an executable file virus or a macro virus. Unprotected access to online services can provide a virus with a springboard into your organisation.

Minimising the Virus Risk

There are several steps you can take to minimise the risk of your organisation becoming infected by a virus and, if a virus does breach your defences, to minimise the risk of data loss.

- Taking regular backups of data on your system is the most important precaution you can take against data loss, whether that data loss is the result of hardware or software malfunction, or virus infection. It is important to ensure that you are able to restore data from these backups. You should also ensure that you have clean copies of all your executable files on floppy disks, these disks should be kept write-protected and stored securely.
- You should scan all incoming software regardless of source. It is a common, though mistaken, belief that shareware, free disks or games are the only source of viruses: while such software can be a source of viruses, it is the origin of the software, NOT the function of software which is important. It's important to remember that viruses have been found on shrink-wrapped software distributed by major companies, and

on disks sent out with hardware. The playing of games is primarily a management issue, rather than a virus issue ‘per se’. For this reason, ALL incoming floppy disks should be checked for viruses.

- The increasing use of email has introduced a new medium for virus infection. As a result all incoming emails that include attached executable code (Programs and Documents) should be scanned for viruses, either on the workstation machine or by a mail gateway that processes mail before the recipent receives the message.
- Floppy disks are a common means by which viruses are spread. Judicious management of workstations, particularly in relation to the use of floppy disks, can help to minimise the risks of infection by boot sector viruses.
    - *Cultivate the habit of write-protecting floppy disks, wherever possible, to prevent virus infection.*
    - *Discourage users from leaving floppy disks in the drive when PCs are switched off, to prevent PCs from being inadvertently booted from a floppy disk infected with a boot sector virus.*
    - *If users do accidentally boot from a diskette, encourage them to power-off and re-start the PC, rather than continuing the boot process.*
    - *Change the CMOS setting of PCs, so that they boot in the sequence to prevent the PC from booting from a floppy disk.*
- Judicious network management can go a long way towards preventing the infection of files stored on a network. As far as normal network users are concerned, a file server is simply a hard disk at the end of a cable: it may be where their software is run from; it may be where their data files are stored; and it is the place to which their files go on their way to the printer. The system administrator can do a lot to protect a network against the possibility of virus infection, simply by making use of the built-in security features offered by most network software. When a user logs-in to the network, the network software checks, by means of a password, to see what rights have been assigned to that user by the network supervisor. If there is a virus memory resident on that user's PC, it has only the same rights as the logged-in user. By setting files to ‘execute-only’, the network supervisor can ensure that users are able to run software without being able to change it; and if the user is unable to change software, then so is the virus this may also be done for data files, by setting them to ‘read-only’. So the system administrator should work along the lines or the user has minimum access and privileges on the system as required to perform his/her job. The situation is different on the workstation itself: here the user is able to change file attributes,

using routines made available by the operating system; and if the user is able to do this, then so is any virus which is memory resident on that user's PC.

Anti-Virus Tools

It is important that your organisation is equipped with the right tools with which to implement an effective anti-virus strategy. Such a strategy should be based on the prevention of virus infection, the earliest possible detection of any virus which breaches your organisation's outer defences and, should a virus spread within your organisation, recovery and a return to normal business as quickly as possible. You should consider the following when selecting which tools to use.

The tools described below are designed both for **prevention** and early **detection** of viruses.

- If a 'sheep-dip' or 'footbath' PC is used to check incoming floppy disks and CDs, this will provide early detection of a virus, before the infected floppy disk or CD is used within the organisation's main system. The 'sheep-dip' PC should be stand-alone to avoid the risk of a virus infecting the network. When using of the this method of protection requires operator vigilence during screening. In a large organisation, it may be advisable to use several 'sheep-dip' PCs one per building, one per department, etc..
- PCs should be protected with an on-access scanner, to provide the first layer of protection 'in-depth' rather than at the perimeter. The on-access scanner runs in the background and will scan disks and files before they are used. The user will be given a pop-up warning, to identify the virus; and the user will not be able to use the infected disk or file. Using an on-access scanner to provide protection for floppy disks, local hard disks and network drives. Usually they are fully-configurable, to enable greater or lesser security for example, checking files which are written to disk may be selected for those PCs which are downloading software, documents, etc. from a remote location the Internet, BBS, etc. Some on-access scanners may be configured to auto-disinfect, so that disks and files may be cleaned automatically, on detection. This makes anti-virus management easier as virus removal is carried out automatically, rather than by a member of an IT Department. You should also configure to log all virus incidents, allowing the IT Department to monitor all virus incidents.

- Network servers should be effectively protected programs and documents may be located on shared network drives; if they become infected, a virus will be able to spread via the network. At the very least, network drives should be scanned regularly from a system administrator's PC. When carrying out this task the administrator's PC should be confirmed as clean before carrying out the scan also the administrator should have an account with only Read-Only access under which to perform the network scan. However, server-based protection for Novell NetWare and Microsoft Windows NT servers are available and should be used; that is, anti-virus programs are designed to run directly from the server. This adds a second layer of protection 'in-depth'. It also makes it easier to manage anti-virus protection, since scanning of network drives and other functions, such as distribution and configuration of anti-virus programs, logging of virus incidents, virus alerts, etc. can be automated.
- The increased use of email systems and the threat from email attachments means that a virus can spread very quickly throughout an organisation. If an organisation has an emailemail connection to the Internet, this threat increases dramatically. Although on-access scanners will prevent access to infected email attachments, this still leaves the logistical problem of removing the infected email attachment from the mail-server and the possibility of an unprotected workstation becoming infected. This risk can be minimised by scanning email as it enters or leaves the organisation. There are types of scanner that are able to scan SMTP mail. Some systems like Lotus Notes/Microsoft Exchange require special scanners that are able to scan email and databases as these are proprietary systems. If email is filtered in this way, it reduces the risk of a virus reaching any of the workstations. This adds an additional layer of protection, at the perimeter.
- If the worst happens, and a virus does get through your defences, it is important that you are able to recover from the infection with the least possible disruption to your organisation's normal business. The following should be considered as essential.
  - Booting clean. Remember that most viruses are memory resident programs. Before attempting to remove these viruses, it is essential to clear memory and boot the PC without loading anything from the hard disk. Booting clean is essential, but it is not as straightforward as it may appear at first sight; for this reason, this subject is dealt with below.
  - Original copies of your applications. If your executable files cannot be disinfected, you will need to delete any infected files and replace them with good copies.

- A backup of the data on your system. If a virus has damaged any of your data, you will need to restore the data from a backup. The most important asset of your organisation is the data; so regular backups should be an integral part of your normal support operation.
- Also use any option within your backup software to perform a virus scan prior to backup or perform a virus scan berfore starting the backup job if this feature is not available.
- Perform a scan of data once it has been restored to ensure the files where not infect prior to backing up.

Booting Clean

NEVER attempt to carry out a clean-up operation if there is a virus in memory. ALWAYS power-off to clear memory and boot from a clean disk, to avoid running anything from the hard disk.

It is wise to ensure that you have a system disk for PCs within your organisation. However, you should consider the following.

- Your DOS system disk should allow you to access the hard disk of PCs running any version of DOS within the organisation. This may mean creating several system disks.
- You may need to load one or more device drivers in order to access some PCs in your organisation for example, if the PC is compressed using Stacker, SuperStore, etc.. If this is the case, your system disk should contain clean copies of these device drivers; and you should create a CONFIG.SYS with the commands necessary to load them.
- If you have a network, you should create a disk containing clean copies of the relevant network drivers; to enable you to connect to the network without running any programs from the network.
- Check the machine's CMOS settings, to ensure that drive A is installed (Exebug virus, for example, removes the CMOS entry for drive A, thus forcing a boot from drive C:. The virus loads into memory from the partition sector and re-installs drive A.

Your system disk(s) should be created in advance of any virus outbreak; a clean-up is not the occasion to discover that you lack the tools necessary to deal with a virus outbreak. We would recommend that you put together a set of ‘emergency tools’, in advance of any virus infection: these tools should be kept up-to-date by the IT department.

Booting Clean Under Windows 9x

A system disk may be created under Windows 9x, using the syntax

```
FORMAT A: /U /S
```

This will enable the PC to be booted clean. However, it has been found that this is NOT sufficient for removing some boot sector virus infections; in a few cases, an attempt to boot clean in this way causes the PC to 'hang'. In these cases, you should proceed as outlined above, using a DOS system disk. Some virus software include a special boot disk with the virus scanner on it to aid this process. It is important to remember to make sure that the system files written to floppy haven't been infected. It is good practice to create a clean boot disk during the installation of the machine's OS, Windows 9x during the installation process does give you this option.

If the PC is running a version of Windows 9x which uses a 32-bit FAT (File Allocation Table), you will be unable to access files on the hard disk if the PC is booted from a old DOS system disk or a system disk created under a version of Windows 9x using a 16-bit FAT. If you use a version of Windows 9x which uses a 32-bit FAT, you should create a specific system disk for this operating system.

What Users Need to Know

The anti-virus tools deployed throughout your organisation are the most effective means of preventing the infection and spread of a virus. The organisation's 'perimeter defence' minimises the risk of a virus entering the organisation. The organisations 'in-depth', desktop protection operates in the background, preventing access to infected disks and files with minimal input required from the user. Server protection adds a secondary layer of defence 'in-depth'; and makes it easier to administer the anti-virus strategy.

The more your anti-virus strategy can be lifted out of the hands of your users, and the more automated the anti-virus scanning, the easier it will be to manage. Remember that users are fallible; and that, in their eyes, 'the virus problem' is an IT problem.

Nevertheless, any comprehensive anti-virus policy should include guidelines for users, outlining the ways in which they are expected to handle data so as to minimise the risk of infection. You should consider the following.

- The organisation should specify a series of **rules**, defining how data should be handled within the organisation. These rules should be simple and clear, or they will not be read and/or understood by users. They should specify what users must, or must not, do. Examples of such rules might be:
  - only authorised software should be used within the organisation;
  - all virus incidents should be reported to the IT Department;
  - employees should take reasonable precautions to avoid the possibility of virus infection where 'reasonable precautions' means following the specified rules and procedures. It should be considered a breach of company discipline if employees fail to comply with the specified rules and procedures. Remember that if you do not specify such rules, it will be very difficult to take disciplinary action against anyone who wilfully or recklessly breaches your anti-virus defences.
- The **procedures** which employees should follow, when handling data, should be clearly outlined. For example, clear details should be given on how incoming floppy disks and CDs should be checked; and whether this is to be done on a separate 'sheep-dip' PC, or by the users themselves.

You should consider providing some form of **education** for users. It is inadvisable to make such 'virus awareness' or 'security' training too intense; the message should be simple and clear. Users should be made aware of the possible consequences of a virus infection. If users understand the way a virus could impact on them, they are more likely to follow the rules and procedures designed to keep the organisation virus free.

First Rev. July 1997. Last Rev. Nov 1999.