Implementing Anti-Virus Controls in the Corporate Arena

(Version 1.00)

Martin Overton
***Chek*WARE**

Email: *ChekWARE@Cavalry.com*
WWW: ***http://www.arachnophiliac.com/cmindex.htm***

Tel: +44 (0) 1403 241376 or +44 (0) 1403 232937

51 Cook Road,
Horsham, West Sussex,
RH12 5GJ, United Kingdom.

Abstract

When you are responsible for the security of 1,000 to 100,000 PCs, virus outbreaks are getting out of hand, the users won't scan, can't run the TSR scanner or don't care about viruses, what do you do?

This appears to be the scenario in many large corporates.

Many security officers or support staff are given the onerous task of anti-virus strategy, policy, testing, implementation and support. Of these, few have the in-depth knowledge that *really is required* to understand the problem, let alone the solutions. How do they choose the right solution(s)? What are the options?

For many it's a catch-22 situation. If they ignore the problem, they are wrong. If they do something and it fails, they are also wrong! Management just want results.

Viruses are at the very least a nuisance and no matter how 'safe' and 'toothless' a virus it still hits the corporate support budget. Magnify this by the number of outbreaks within a company and add the cost of anti-virus software, updates and training and the problem becomes more focused and expensive.

This paper aims to answer the question that many corporates are asking 'What anti-virus defences do I choose, how do I implement them and how do I know that they are sufficient'.

This paper was written for, and presented at the Compsec '99 International conference at London England on November 3rd - 5th 1999.

I would welcome any constructive feedback on this paper and it's content.
This paper will be updated from time to time.
(Martin Overton 5th November 1999)

The Problem[MGO96]

Before we begin I think it would be worth spending a little time looking at the common problems and some of their solutions.

Background

According to the Information Security Breaches Survey 1996, the most common security breach reported were computer viruses. The most expensive virus outbreak reported during the survey was estimated at £100,000.

By now most, if not all companies have encountered viruses. Their response to this problem is either panic, confusion, anger or in a few cases a well-geared machine kicks into action to solve the problem.

Most companies' anti-virus defence consists of a scanner on the desktop PC[VB-1] and in most cases nothing else is used to combat the virus threat. The ability of most companies to defend themselves against the ever-growing numbers of new viruses is practically nil.

Viruses are now an everyday business problem[VB-2] and that trend will continue to get worse for the foreseeable future.

The Cost

British businesses lost £28 million[1] due to reported virus incidents in 1994. This is just the tip of the iceberg, as many companies do not report virus incidents due to the fear of lost confidence, both from business partners and customers and the subsequent affect on the companies stocks.

Testing

How do you test anti-virus software?

Well, for most corporates, it is simply out of the question. Even if you have several or tens of thousands of viruses on hand *(unlikely)* how do you know they are *real* viruses? Remember that to be viruses they *must* replicate otherwise they are considered germs or more often damaged files.

Even if you do get a valid virus test set, how do you test anti-virus software without risking cross-contaminating your systems?

Do you want to trust the glossy magazines reviews? Of course they rarely use *real* viruses and the journalist doing the test knows little or nothing about viruses. Never mind, the winning products got a great user-friendly interface, that's all you're interested in right?

Well, there's always the anti-virus companies themselves. They are bound to give impartial advice, right?

This is the biggest headache for the corporate security officer!

The answer lies in independent[2] tests carried out by researchers that understand the issues and can in most cases make impartial recommendations on the ability of a scanner or other anti-virus counter-measure.

[1] Source: National Computing Centre Survey 1994.

[2] Such as Marko Helenius of the University of Tampere. Virus Bulletin also perform regular comparative tests, but some feel that they are a little too close to the industry to be completely objective.

Threats

Let's have a quick review of the viral threats that occur in companies.

Boot Viruses

Until recently floppy disks infected with boot and partition sector viruses accounted for in excess of 80% of virus infections reported world-wide. Against all logic boot and partition sector viruses spread faster than most file viruses.

File Viruses

This class of viruses infect executable files, these include the common *.EXE (including *.SCR) and *.COM files to the more esoteric file types such as *.TTF, *.OVL, *.BIN, *.DRV, etc.

Most of this class of viruses either infect a file by one of the following methods, overwriting the start of the file with the viruses code, appending the virus code to the end of the file and modifying the original host to run the viral code first, or pre-pending the virus code to the beginning of the host.

Viruses can be freely found on the internet. However, virus outbreaks linked to the internet sites run by commercial companies are quite rare[3]. Most site operators have a good policy of checking files for viruses before offering them for downloading to the public. This is similar to most well run Bulletin Board Systems and similar information systems

Be more worried about e-mail that contains binary data, such as Word and Excel files (Yes, they are binary files!) to be the biggest threat the internet has to offer corporates. This is of course only true for viruses and Trojan horses, other security issues for internet use need to be similarly addressed.

Multipartile Viruses

This is a class of viruses that infect boot/partition sectors and files. In many cases the virus can be spread via infected floppies, like boot sector viruses, and via infected files as with executable viruses.

Y2K Viruses

"There are no known viruses that trigger on 1st January 2000, at this time."[4]

According to a number of anti-virus vendors there are currently no known viruses that have a trigger date of the 1st Jan 2000. Bear in mind that between 300-800 new viruses are discovered each and every month. Of these, only a small percentage of viruses are reported in the wild.

There is certainly a risk that a virus (or a number of them) will be written targeting that date, these will most likely be released shortly before the 1st Jan 2000. The most likely scenario will be a number released throughout December to cause maximum confusion and disruption.

[3] Although a number of large companies have inadvertently placed infected files on their web sites. These include Microsoft.

[4] This statement was known to be true as at 5th September 1999, although there are a few viruses that will trigger on the 1st of Jan of any year.

Macro Viruses

Macro viruses have become the biggest virus threat to corporate security. What was once considered safe, is now seen as just as capable of carrying an infection as executable code[5]. Indeed, the boundary between data and executable code is getting mighty blurred. Currently Microsoft Word for Windows (6.0, 95, 97 and 2000), Excel 4.0, 95, 97 and 2000, PowerPoint 97 and 2000, Access 97 and 2000, Lotus Wordpro (*was AmiPro*) can be infected by this class of viruses. Even more worrying is that other vendors are including VBA into their products. Already Visio includes VBA and the latest version of WordPerfect Office now supports VBA too.

Of course many applications have macro languages built in to them to give even higher functionality to the end-user. Many are mini-operating systems in their own right. What this means to you is that macro viruses are going to become the number one threat to your corporate data. So expect the worst, if you use a widely used application with a macro language expect it to be targeted sooner rather than later.

Macro viruses pose a higher threat than the more conventional viruses for several reasons:

- They spread through any means used to share documents, diskettes, e-mail and groupware.
- They execute on any operating system that runs the application and the macro language that the virus runs under.
- The potential for damage, both from destructive variants, such as Hot and from the ease of creation by disgruntled employees.

Trojan Horses

The difference between viruses and Trojans is frequently argued, but as a general rule of thumb, the difference can be simply summed up thus:

Viruses must replicate to be classed as viruses and Trojans don't replicate.

A Trojan Horse is a program that does something that its programmer intended but the user is not expecting.

Worms

Worms have made a comeback over the last year, but just what is a worm and how does it differ from a virus and a Trojan?

A worm is a program that makes copies of itself, for example from one disk drive to another, or by copying itself using email or some other transport mechanism, such as the network. It may do damage and compromise the security of the computer, but it doesn't replicate by changing a hosts code or files.

Windows Scripting Language (VBS)

This is a relatively new threat and currently only effects Windows 98, NT 2000 and other operating systems that have installed Windows Scripting support (this is a option that can be installed as part of Internet Explorer 5.0).

[5] Macro Viruses first became a reality in 1995, although the possibility of macro viruses was known a number of years before.

Java

We have now seen the first Java virus[6], and there are a number of malicious applets now known. The original Java specification meant that an applet could not access the file system on a host system as it was forced to run in its 'sand box'. However due to some holes the applets could be programmed to break out of the 'sand-box'. Luckily most of these holes have now been fixed, but new exploits come to light from time to time.

Active-X

The simplest way to describe Active-X and the threats it brings is to compare it to standard *.EXE files (which it basically is, just renamed). Just like any other executable file it has the same rights to the operating system that you do. So it could format the hard disk, delete files, copy data to a remote site, or even steal password or credit card information.

Support staff

Support staff are frequently guilty of infecting PC's that they are supposed to be fixing, all be it unintentionally. Nevertheless, support staff are a high risk category and should be treated as such.

Engineers

Engineers should also be treated as a high risk category. More so if they are from third party maintainers as the possibility of them encountering a virus is many times greater than those of internal engineers.

Cover disks

The ubiquitous magazine cover disk is still to be considered as much as a viral threat as 'Typhoid Mary'. Don't forget that cover CD-ROMs can also carry viruses and virus droppers, scanning 560MB of CD-ROM can take some time, but at least your staff at can't infect them![7]

Home PC's

Many of your staff, especially your IT staff will have computers of their own at home. These can be another source of virus contaminated files and disks coming into your company. It makes sense to expand your anti-virus protection to included these home systems, as in the long run it will lead to lower instances of viruses being brought in from home.

Solutions

We've identified the problems and threats, now let's examine some of the solutions.

"Virus scanners are only as good as their latest update"

One thing you should be aware of is that there is no 100% solution to the virus problem. Any company that informs you that their product offers 100% protection from viruses are either naive or just don't fully understand the real problem.

However if you approach the problem in the right way, then you can minimise the percentage gap from that perfect 100%. A well-designed approach can be expected to give a 98-99.5% protection from viruses and their effects.

[6] StrangeBrew.

[7] Of course this cannot be said to be true for CD-RW or CD-W drives and writeable media.

Policy

Use the K.I.S.S[8] approach for your anti-virus policy. The reason for keeping it simple is so that your staff can remember it. Something like the following would be sufficient as a basic template:

Sample Anti-Virus Policy

1. **Use the anti-virus software provided.**

    - *This is part of your terms and conditions of employment.*

2. **Report any virus detected to security on ext. xxxxx**

    - *Do not use your PC until directed to.*
    - *Do not let anyone use any of your disks.*

Education

You may think that trying to educate your staff about the risk of viruses is like trying to nail jelly to a wall, and about as rewarding, and in most cases you are right. Your non-IT staff will generally be either blasé, paranoid or simply ignorant about viruses. They simply see it as not being their problem.

Support staff

In many corporates, your support staff are the ones that get the first call from a panicked user who has just been informed by the anti-virus software that the "*XYZ123 Virus Has Been Detected .....*". Therefore they need to know what a virus is, how to remove it correctly, and how not to overreact[9].

It is also of little use if only one member of the team has "*the knowledge*" as you can almost guarantee that the virus will be found when they are:

1. *Off sick.*
2. *On holiday.*
3. *On a course.*
4. *No longer working for the company.*

To avoid this very common pitfall, simply spread the skill around the team(s)!

Developers

Your application developers can be seen as major players in the league of 'viral spread'. They must be accountable for the master copies of software that they produce and be fully aware of the disastrous impact of them sending an infected master program or diskette for duplication. This is even more important where external companies may receive the infected application as a lawsuit may quickly follow.

End users

These make up the bulk of most companies, and there lies the problem! The IT staff may understand about viruses, but non-IT staff just want to get on with their work.

---

[8] **K**eep **I**t **S**imple **S**tupid

[9] Also known as 'Headless Chicken Mode'.

Any form of anti-virus needs to be fast and effective or they won't want to use it and in some cases may actually remove the protection that you have installed.

You need to make the protection as invisible as possible

Multi-Layered, What's That?

A multi-layered approach involves the use of multiple technologies for virus detection.

"But why do I need to implement a multi-layered approach?"

Below are the main reasons for using a multi-layered approach:

- *New viruses appearing more rapidly on business PCs. (300-800 new viruses every month!)*
- *Virus GLUT (many virus scanner producers are finding it tough to keep up).*
- *Scanners can only detect viruses that are known to them.*

Any one anti-virus technology will not offer 100% protection from all viruses and other malware. A Multi-layered approach would include at least several, and in some cases most of the following anti-virus technologies:

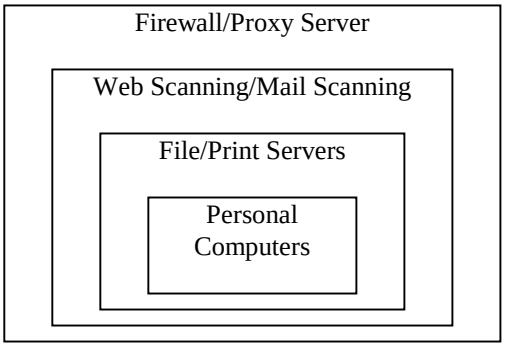
- *Signature scanning*
- *Code emulation*
- *Integrity checking*
- *Heuristics*
- *Interrupt tracing*
- *Decoy launching*
- *Diskette authorisation*
- *Behaviour blocking*
- *REGULAR BACKUPS*

Multi-layered protection is the *'belt-and-braces'* approach to the virus problem. Caution must be exercised as each extra layer can carry an increased support burden if the wrong products are chosen.

Yes, regular backups of DATA on your system is still very important, you can replace program files easily enough from master disks, but corporate data is worth a lot more to your company and is very hard to replace if damaged or destroyed.

So what is the answer? Well, look at the problem as a number of layers, or perimeters that need to be protected.

Most companies only protect their PC's and consider that is all they can do to protect themselves. However the hardest part of relying on this old model is that updates to all the PCs in the company can take far to long, allowing a virus to establish a serious beachhead.



However if you have a centralised e-mail[10] backbone and/or Firewall/Proxy, then to add protection from a new virus is significantly easier, as you only have a small number of systems to update[11].

[10] According to the Gartner Group, E-Mail is responsible for 40% of virus outbreaks, and that figure will grow as more companies spread the use of e-mail and products that use Microsoft VBA.

The same advice applies to the next layer in; your file/print servers. If you stop the viruses getting onto the servers in the first place then the spread of any virus that gets in is severely limited.

Desktop and portable PCs should not be ignored, as they still have a part to play in the overall virus protection plan for any company, but by using this multiple-layers approach you can help to minimise the chance of a virus getting into your company, and even if it does the infection should not spread too far before it gets noticed by another layer of the model.

Even with this 'belt-and-braces' approach you will still only get 98%-99.5% protection from viruses.

Multi-Level, What's That?

Do all you users have the same shoe size, dress sense or sense of humour? Of course not. Likewise their exposure to viruses are also different.

How do I categorise my staff?

Your highest risk users are frequently your support staff and your system and application developers. Don't forget your business critical departments in this risk category. Why? Well, what happens if you get a major virus outbreak in a department that brings in a large slice of the revenue for your company? Can you afford to lose business for hours or days?

Well, What Should We Use?

Products

Do you really expect me to tell which suppliers' products to use? Well just have a look at some good independent reviews to help you choose a brand. Don't forget to check out the support structure for the company that you choose. Do they cover all 365 days of the year? How often do you get updates? Can they handle new viruses that you find and supply detection and cleaning methods promptly?

Below are the major categories of anti-virus software that you might want to include in your multi-layered virus protection.

Scanners
Integrity Checkers
Behaviour Blockers
Diskette Authorisation
Access Control

[11] This approach proved very successful with Melissa, enabling one company to remain completely free of infection from this virus and the numerous variants that followed. Mail was simply refused entry when the mail scanner detected the virus.

Example Multi-Layered Approach Product Table.

Platform	Criticality			
	High	**Medium**	**Standard**	**Low**
DOS	***1a or 1c 2a or 2b or 2c 3a***	***1a or 1c 2a or 2b***	***1a***	***1d***
Windows 3.x	***1b and 1f 2a or 2b or 2c 3a***	***1b and 1f 2b or 2c***	***1b***	***1a (Scheduled)***
Windows 95	***1b and 1f 2a or 2b or 2c 3a***	***1b and 1f 2b or 2c***	***1b***	***1a (Scheduled)***
Windows NT	***1a or 1b or 1c and 1f 2a or 2b or 2c 3a***	***1a or 1b and 1f 2b or 2c***	***1a or 1b***	***1a (Scheduled)***
OS/2	***1a or 1c 2a or 2b or 2c 3a***	***1a 2b or 2c***	***1a (Scheduled)***	***1a (Scheduled)***
Novell Netware	***1e 2b***	***1e***	***1e***	***1a (Scheduled)***
IBM Lan Server / Microsoft Lan Manager	***1a (Scheduled)***	***1a (Scheduled)***	***1a (Scheduled)***	***1a (Scheduled)***
Mail Gateway/ Groupware	***1a or 1b or 1c and 1f 2a or 2b or 2c***	***1a or 1b and 1f 2b or 2c***	***1a or 1b***	***1a (Scheduled)***
Proxy Server or Firewall	***1b or 1c and 1f 2c***	***1b and 1f 2c***	***1b***	***1b***

1a. On-demand scanner
1b On-access scanner[12]
1c. Heuristic scanner
1d. TSR Scanner
1e. NLM scanner
1f. Macro scanner
2a. Diskette Authorisation
2b. Integrity checker
2c. Behaviour blocker
3a. Access control

Below are some examples of how to categorise your staff:

High Risk

Support staff, Engineers, Developers, Critical business areas, Staff with a history of virus outbreaks and areas with large diskette or document throughput.

Medium Risk

Users not in the above category, but that have a high throughput of diskettes (>10 a day) or files from applications that use macro languages.

Standard Risk

This is your standard level of anti-virus protection.

Low Risk

The level of protection for PC's that are rarely changed, such as print servers or gateways.

[12] 95 or 98 VxD or NT Service.

Free Protection!

Who says there is no such things as a free lunch!

Novell Netware

There are some very simple but highly effective ways that you can limit the spread of a file infecting virus on a Novell server. These are:

- Do not use CREATE and WRITE permission for any directory that contains executable files. This is especially true of PUBLIC and SYSTEM shared directories. Try to default user access to shared directories as:

```
May Read from File      (R)
  May Scan for Files    (F)
```

- Do not allow your support staff to use the SUPERVISOR or ADMINISTRATOR id for normal daily use of the server. Restrict its use to tasks that really require *full* access to the server, otherwise if they introduce a virus onto the server it will probably spread very rapidly to the whole network and even infect the workstations. Of course allow their *normal* user id to have full server READ access, but on no account allow them WRITE access outside their own user area [Sophos1].

- Do NOT use the EXECUTE ONLY Novell attribute for files as although this is very secure, it will even bar file access to a virus scanner.

PC's

- To provide simple but very effective protection from true boot and partition sector viruses, simply change the BIOS boot sequence from **`A:, C:`** to **`C:, A:.`**

  Now even if an infected diskette is left in the drive during a reboot or power-up then the system is unlikely to become infected.

- Otherwise, removing or disabling the floppy drive will help, but this is probably overkill.

Implementation

Now let's look at the final piece of the puzzle, you've chosen your protection methods, you have your policy in place, now how do you implement it all?

Let's get one thing straight right now. You will not achieve 100% coverage of your installed base; the best you can hope for is 90-95%[13]. There are a number of vendors that now offer their own management tools to implement and auto-update their products, as well as the more generic products such as: Intel Landesk, Microsoft SMS, Novell ZenWorks, and others.

With these products you have often have two methodologies to use: ***Pull*** (let the client poll the server and 'pull' the update/installation down from the server) or ***Push*** (get the server to Push the update/installation to the managed clients).

There are arguments for both Push and Pull methodologies, so choosing one is up to you.

[13] The more computers you have in your organisation the greater the change for the percentage of coverage to be lower, especially if you have users that have portable computers, as these are frequently the hardest to update because of their very portability.

Network

Installing anti-virus tools on to a network and then getting the workstation to run them from there is a sensible solution. It enables central control of both updates and where required installation of anti-virus software for all the users of the network server that they login to.

The example below assumes a Novell Netware server and a mixture of OS/2, Windows (3.x, '95 and NT) and DOS workstations.

The directory structure on the server looks like this:

```
VOL1:\ANTIVIR
                    \DOS
                    \WIN3
                    \WIN95
                    \WINNT
                    \OS2
```

For each of these directories a Novell Group would need to be created and all the users of each operating system would need to be added to the relevant group. This can then be used to run the correct software automatically when the user logs in to the server.

The system login script would then be edited to check to see which group a user is in, as below:

```
IF MEMBER OF "WIN95" THEN
      #COMMAND /C WINSCAN.EXE
END
```

Some of the better products have utilities to make installation and updating of files easier. This is especially useful where a VxD or NT Service based scanner is used as the files will almost certainly need to be installed / updated on the local workstation's hard drive. A test for the presence and version can be automated in a similar fashion to the example above for calling a scanner directly during the login script.

A central code server needs to be created so that other LAN Supervisors or Administrators can login and copy the software or updates at regular intervals. The copying of updates to the other satellite servers could also be automated. Once setup this is a very efficient solution with a very low total cost of ownership compared to individual workstation updating via diskettes.

Similar automation routines can be used for other network operating systems such as Lan Manager or Lan Server, Windows NT, etc.

Standalone

This covers the shrinking number of isolated (un-connected to LAN) PC's. These could be handled in a number of ways:

- An automated floppy installation.
- Via E-Mail attached as a binary attachment, such as Lotus Notes, CC: Mail, MS Mail or Internet[14] Mail.

[14] This requires converting the file to MIME or UUENCODED format for internet transmission.

Done! What's Next?

Well, you have now installed your chosen anti-virus software, all your staff are running them, you are scanning e-mail and possibly even web content, and you are surely fully protected from viruses now?

Yes, you are now protected from known viruses and if you have implemented a multi-layered approach then also from most new or modified viruses that the scanner doesn't yet know about. Now though, is not the time to think that the war is won? This is just the first skirmish in the never-ending war against viruses.

To continue winning as many rounds as possible, these are the points that you must consider:

- Frequency of scanner updates.
- Pro-active approach.
- Review your strategy and products at least yearly.
- Evaluate new technologies as they appear.

Conclusion

Conventional virus scanners just on the desktop are still needed for identification of known viruses. However, they are no longer strong enough to offer protection from the ever-increasing numbers of new viruses that are appearing 'in-the-wild' *before* most desktop scanners can detect them, due to the time it takes updates to propagate throughout a large organisation. A multi-layered approach for protection from viruses *is* the way forward (both in terms of type of detection products and multiple layers of detection zones (desktop, server, mail, firewall/proxy)).

Virus scanners should still be used for checking floppy disks, CD-ROM's and downloaded files before they are used, or a VxD or NT Service based scanner should be used to give similar automatic protection. Other technologies must be used to help strengthen the defences, especially in answer to the macro virus problem as this has the greatest scope for impact in corporates.

The desktop is not the only place that detection needs to be implemented, you should seriously consider e-mail scanning and the growing threat of mobile code may soon warrant web scanning at Firewall or proxy level to minimise the threats from malicious mobile code.

There are a number of new threats expected in the next few years and these will make the lives of the corporate security staff even more interesting and challenging.

[MGO96] Martin Overton - Anti-Virus in the Corporate Arena, Proceedings of the 1996 Virus Bulletin International Conference.

[VB-1] Editorial, Virus Bulletin February 1994.

[VB-2] Editorial, Virus Bulletin April 1994.

[Sophos1] J. Benjamin Sidle and Dr. Jan Hruska, Viruses and Anti-Virus Measures on Netware.