GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Tommy Flaherty
GIAC Security Essentials Certification
Version 1.4b, option 1.

April 1, 2003

Planning and implementation of an enterprise anti-virus solution

Introduction

In today's corporate environment, the threat from virus infection has become a very serious one indeed. The quality, configuration and implementation of anti-virus protection play a vital role in protecting a company's assets, resources, customer data and the image the company projects to the outside world.

This document will discuss the threat from and defenses used against today's virus technology. It will outline the key components of a strong enterprise-wide anti-virus solution with consideration for desktop, server, and email protection. It will also discuss the planning, implementation, and management of a new anti-virus solution.

Just how destructive are viruses?

- According to details published by Internet Security Systems, "The May 2000, "I Love You" virus cost businesses an astonishing $6.7 billion in lost productivity and repairs." [1]

- A report published by the British Department of Trade and Industry in 2002 stated that,

> Recent high profile international virus attacks (such as Nimda and Code Red blended threats – viruses that possess characteristics of worms, viruses and Trojans and blend these with hacking techniques) forced many UK businesses to shut down external connections to the internet, and the cost in terms of lost business, staff time and downtime ran to millions of pounds. [2]

- An article published by iCSAlabs reported that, "The David Smith case and the stipulation (agreement by both prosecutors and defendants) that damages caused by the Melissa virus were in excess of $80 Million, proves that so called "benign viruses" are no where near benign." [3]

There are many more estimates on the cost of virus infection to businesses worldwide. The chances are high that these are actually underestimated. After all, how many companies would want to advertise the fact that any component of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

their network security has been compromised. Making this kind of information public could cause untold damage to market and customer confidence.

If a virus succeeds in compromising a company's private information, the chances are high that the company will not be aware of it. This compounds the issue even further by giving the perpetrators additional time to use the illegally obtained information.
In essence, today's technologically advanced virus threat can be seen as a 'automated hacker'. This virus can contain multiple components that take it through the different stages from infiltrating an organization to finding critical information, and finally passing the information back to the source of the virus.
'Section A' provides details on the virus threat and the various forms it can take.

Section A: The threat
Today's viruses have the ability to steal business-critical information and pass it on to unscrupulous individuals who then use that information to steal from a company or its customers.
The threat manifests itself in a number of different of ways.

- Viruses.
- Worms.
- Trojans.
- Hackers (Crackers).
- 'Blended Threat'.

Virus
SearchSecurity.com defines a virus as follows: "A virus is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. A virus is often designed so that it is automatically spread to other computer users." [4]

The preceding definition of a virus was taken from the Internet in February of 2003. The definition only goes a small way in describing just how dangerous and technologically advanced, today's viruses have become. In the twenty-first century, the virus threat has taken on a completely different role with the potential to cause far- reaching damage resulting in the loss of business for many companies.

A good example of the danger presented by virus infection is the 'W32.Funlove.4099' virus. This virus performs a number of functions including infecting files with .exe, .scr and .ocx extensions. There are two very unique and highly dangerous features to this virus. First, it will try to start itself as a service on Windows NT machines. Second, it waits until someone with administrative privileges logs on, and then modifies the 'NtosKrnl.exe' file, at which point it can give full rights on any file to any user.
Full details on the virus can be found at:
http://securityresponse.symantec.com/avcenter/venc/data/w32.funlove.4099.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Worm

SearchSecurity.com defines a worm as follows: “A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.” [5]
Today, one of the most well known types of worm is the ‘mass-mailing worm’. As the name suggests, this type of worm is usually distributed through email. One of the most famous of the ‘mass-mailing worms’ is the ‘ILOVEYOU’ or “LoveBug’ worm. To propagate itself, the worm mails itself to everyone in the user’s Outlook address book. It also downloads a ‘password-stealing Trojan’, which emails all passwords found to ‘mailme@super.net.ph’.
Full details on this virus can be found at: http://www.f-secure.com/v-descs/love.shtml

Trojan horse

SearchSecurity.com defines a Trojan horse as follows: “In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk.” [6]

‘Backdoor.SubSeven’ is a classic example of a Trojan. It has the ability to enable unauthorized people to access an infected computer over the Internet without the user’s knowledge. Once the infection is successful, this Trojan can do almost anything on the computer from setting up an FTP server to browsing files, to restarting the computer.
Full details on this Trojan can be found at:
http://www.symantec.com/avcenter/venc/data/backdoor.subseven.html

Hacker (Cracker)

SearchSecurity.com defines a hacker as follows: “Hacker is a term used by some to mean "a clever programmer" and by others, especially journalists or their editors, to mean "someone who tries to break into computer systems." [7]
The definition given by SearchSecurity.com for a cracker is similar: “A cracker is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security.” [8]

It is said that the main difference between a hacker and a cracker is supposedly their motive(s) for breaching security. Hacker’s supposedly breach security just to see if it can be done, or to highlight inadequacies in the security configuration. Crackers supposedly breach security to do damage or to steal confidential information. From a security perspective, whatever their motive, both hackers

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

and crackers must be viewed as a security threat. All appropriate measures should be taken to prevent them from breaching your network.

Note: Since the focus of this document is to discuss virus activity and how to protect against it, there will not be an in-depth discussion of hackers or crackers. The term 'hackers' will be used for any future reference to hackers or crackers in this document.

Blended Threat

The 'Blended Threat' is a combination of two or more of the previously mentioned threats. It uses these in conjunction with operating system and/or application vulnerabilities such as 'OS' service or web browser vulnerabilities. This is one of the most serious security threats to appear in recent years. What makes it so difficult to defend against is the fact that it can attack a system from multiple access points to infiltrate security.

W32.Bugbear is a good example of this type of threat. Although it is a 'mass-mailing worm', it includes a Trojan that can log keyboard strokes to steal passwords, and another Trojan that open's a backdoor port to listen for commands from the hacker.
Further details on W32.Bugbear can be seen at:
http://securityresponse.symantec.com/avcenter/venc/data/w32.bugbear@mm.html

Now that we have some more specifics on the threats and their numerous sources, we can examine the most common methods of defending against them.

Section B: Defenses

What can be done to combat today's virus threat?

There are four main defenses against this threat.

- Anti-Virus software
- Content Filtering Software
- Intrusion Detection Systems
- User Education

Anti-Virus software

Anti-Virus software is now an integral part of most computer installations in the corporate environment. Businesses have realized the vital importance of having this type of product installed on all computers in the enterprise.
The technology behind the software has had to evolve at an incredible rate to keep pace with the latest virus threats. The average anti-virus product today has virus definitions for over 60,000 different types of virus including worms and Trojans.

Today's anti-virus products have many configurable options for detecting and dealing with a virus. These range from specifying which files should be scanned for virus infection, to what actions to take with 'macro virus' infections. Another

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

important feature is ‘Heuristics’. Heuristics has the ability to monitor for activity that a virus might typically perform. This gives an additional layer of protection against ‘unknown viruses’ that the AV product does not yet have a virus definition for. Care must be taken when using this option as it can use up a lot of additional computer resources and if configured incorrectly, can lead to many ‘false-positive’ virus alerts.

Content Filtering

Content filtering software is used to block or filter specific items. This could be anything from blocking emails with inappropriate language, to blocking access to non-business related web sites. This type of product can usually perform message header scanning along with numerous other scans for ‘non-virus type exploits’ that anti-virus products do not yet have the capability to detect.
Some anti-virus products today have some basic content filtering capabilities such as ‘keyword searching’. However, the current trend seems to be leaning towards vendors adding anti-virus scanning capability to their existing content filtering products.
A description of Content Filtering can be seen at:
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci863125,00.html

Intrusion Detection Systems

Intrusion Detection Systems provide security management for computers and networks. This type of product monitors many different areas of the computer or network for ‘unusual behavior’. The ‘unusual behavior’ covers many areas including user/computer activity, file changes, policy change/violations.
A description of Intrusion Detection can be seen at:
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci295031,00.html

Since the focus of this document is anti-virus protection, Content Filtering and Intrusion Detection Systems will not be discussed in detail.

User Education

The area of user education is often overlooked when planning or implementing security-based products. Unfortunately, this oversight can be very costly. Security-based products such as anti-virus and content filtering software are used not only to protect the user on the inside from outside attackers, they are also used to protect users from themselves.

No matter how good your anti-virus solution is, there will always be certain situations where users will be presented with making a decision on what to do with a certain email or attachment. The attached file may be a new virus that your anti-virus software cannot yet detect. At this point the only thing that will stop this virus is if the user has been educated on how to deal with the suspicious attachment.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

This is where user education comes in. By educating the user community to be aware of the constant threat of virus infection, you can significantly reduce the number of virus infections that have to be dealt with. Details of what this education should include can be seen in “Step 2: Evaluate the current company anti-virus policy” on page 11.

Section C: Points of Entry

As with any type of defense system, the weakest link is also the strongest link. In this case, the weakest links will always be the points of entry for all network traffic. In order to take full advantage of the anti-virus defenses you have, these defenses must be deployed with particular attention to the points of entry in your network. This process can be simplified by grouping like components of the network infrastructure into different tiers.

Following is a breakdown of the main tiers of the network infrastructure from a computer perspective. Included are recommendations for anti-virus protection at each tier.

Tier 1: User Computers

Comprised of all desktop computers including laptops and PDA’s. User computers usually account for the highest percentage of the total computer infrastructure. They also receive data from multiple sources, such as, email, file, HTTP (web traffic), FTP file transfers, CD-ROM and floppy disks.

Anti-Virus protection at Tier 1

Because these devices can receive data from a variety of sources, this tier is highly vulnerable to virus infection. Another important reason for optimum anti-virus protection at this level is that certain file/data types cannot be virus scanned anywhere else in the tier structure until they get to this tier and are opened by the user. An example of this would be encrypted data coming from an SSL source. Encrypted files cannot be virus scanned until they arrive at the destination computer and are decrypted when the recipient opens them. Therefore, scanning this type of file at the Firewall or other gateway server would not yield the presence of a virus.

Note: Some newer content-filtering solutions have the ability to allow all, none, or some encrypted emails to pass through.

Tier 2: Local Servers

This tier sits above the user computers and usually contains user and/or application data and other network-shared resources.
Local servers are usually comprised of three main types. File Servers, Application Servers and Print Servers.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Anti-Virus protection at Tier 2
Local servers are the main repositories for all user data saved on the network. Anti-Virus protection at this tier is very important in protecting existing data, and any new data saved here from desktop machines or other sources.

The following is a simple scenario that illustrates the vital importance of having anti-virus protection at both the desktop and server tiers.

If a desktop machine does not have a fully functional anti-virus product installed, and an infected file is copied from the desktop to a server, the virus will be detected at the server, and appropriate action taken. This scenario could also be applied in reverse order with the desktop detecting a virus copied down from the server.

Tier 3: Messaging Servers
This tier sits at the same level as the Local Servers and contains user mailboxes and public folders. It routes email to internal and external addresses.

Anti-Virus protection at Tier 3
Messaging servers hold all employee email, which is stored in individual mailboxes. Because of the nature of a lot of today's email-aware viruses, it is crucial that a fast, high-quality email anti-virus scanner be running on all email servers.

In general, email servers do not transfer non-email type data back and forth to user computers. However, exceptions to this would be the administrator(s) of the email system, or a hacker inside the network with access to shares on the email server. Consequently, anti-virus protection is also recommended for the email server operating system and file system.

Note: When installing anti-virus software on any server that has any kind of database running, it is vital to confirm whether the database supports being scanned by the anti-virus product. In the case of the databases for Microsoft Exchange and Lotus Domino server, 'non-email aware' anti-virus products must be setup to exclude these databases from scanning. Not setting this exclusion can cause serious damage to the mail server database. Only 'email aware' anti-virus products should be allowed to scan the mail server databases.

Tier 4: Gateway Servers
This tier is usually the outer most point of contact for all traffic in the enterprise.

Anti-Virus protection at Tier 4
The right products running on gateway servers can detect viruses in almost any format. In this way they can provide the following benefits:

- Reduced workload on email servers, user computers and local servers by eliminating the virus before it reaches them.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Reduced risk of virus infection by providing an additional layer of anti-virus protection. This would safeguard against the possibility that for any reason, the virus scanner at the email server or user computer was malfunctioning or not up to date.
- Contributes to layered multi-vendor approach to anti-virus protection. In rare cases, illustrated in some anti-virus lab tests, there are instances where specific anti-virus products do not detect specific types of viruses. If that particular product were in use right across all the tiers, the virus would have complete access to the network. This situation could be prevented from occurring by having an additional vendor product at any one of the tiers.

Tier 5: Users

As discussed in 'Section B: Defenses', the user community is often responsible for making the decision on what to do with a suspicious attachment, or embedded link in an email.

When creating many of today's viruses, the creator's put a lot of thought into how best to tempt a user's curiosity. One of the virus creator's goals is to make curiosity override common sense. The result being that the user may be tricked into performing an action they normally would not. Graham Cluley states that, "Viruses such as the Love Bug, Anna Kournikova, Sircam and Magistr do not rely on technical flaws to distribute themselves, but rather take advantage of the weaknesses in human nature." [9]

These viruses could in fact be seen to be using a type of 'Social Engineering' to lull users into a false sense of security. Social Engineers rely heavily on human interaction to assist in opening the door to a company's private information.

Why use layered multi-vendor anti-virus protection?

One approach to anti-virus protection in an enterprise environment is to utilize multiple vendor anti-virus products at the different tiers of the network/computer infrastructure, or to use a single vendor product that can incorporate multiple scan engines.

Note: Multiple scan engines in one product are more commonly available for messaging anti-virus products or gateways.

The theory is that multiple vendors will provide a layered approach to the anti-virus threat, maximizing the likelihood that, if a particular virus or threat is rare, at least one of the vendors will catch it before it can spread within the network. In a perfect world, one vendor would have all the anti-virus products a company needs. In reality, this is often not the case.

Leaning on this methodology, a number of anti-virus vendors have in recent years, developed products that can utilize two or more anti-virus scan engines

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

from different vendors. The link below explains why one such vendor, 'GFi', feels that "no single anti-virus engine can fully protect against all possible threats." http://www.gfi.com/mailsecurity/wpmultiplevirusengines.htm
Some of the tests described in the article highlight the fact that some AV products do not support scanning files using specific types of compression. Other products may scan but will fail to detect a virus in files using specific types of compression. Another issue that is not mentioned in the GFi article is that when a new virus threat is released, all anti-virus vendors will not have a new definition for the virus at the same time. Although the time difference can be minimal, this still leaves a 'window of opportunity' for a new virus to infect the enterprise.

Steps in planning the solution
Keeping the previous information on 'multi-tier' and 'multi-vendor' protection in mind, we can now move on to the planning stages of the solution. For the purpose of illustration, a fictitious company called 'The Wide Open Corporation' will be used.

Following is an overview of the main steps involved in planning the solution followed by a breakdown of each step in the process.

1. Determine what the company needs in an anti-virus solution, looking at all aspects of implementation, ease of management, features and performance of the product(s).
2. Evaluate the current company anti-virus policy. Does the company have a policy? If not, this is a perfect time to draft one. Details of what the policy should contain will be discussed further on.
3. Evaluate the existing anti-virus solution focusing on maximizing its configuration, or, if necessary, replacing it with a product(s) that more closely matches the company needs as defined in step 1.
4. If the evaluation determines that a replacement is necessary, lay the groundwork for evaluating the 'best alternatives' available. In order for the evaluation of alternatives to be successful, step one must be completed with great attention to detail. This will make it easier to eliminate products that do not meet the company needs, saving valuable time for the project.
5. Once the available products have been narrowed down to a manageable number, these products should if possible, be tested in a 'lab environment'. NOTE: To avoid major issues in a company's production environment, it is strongly recommended that all software testing of any kind be completed in a non-production or 'lab environment'.
6. Once product(s) selection has been accomplished, a detailed implementation plan is vital to the success of the new product(s).
7. Implement the new product(s).
8. Perform a regular review of the current anti-virus solution. As the company changes over time and most likely grows, does the product(s) still meet all the needs of the company? Monitor for new products in the marketplace that might better suit the changing needs of the company.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Step 1: Determine what the company needs in an anti-virus solution
This step will look at all aspects of implementation, ease of management, features and performance of the product(s).

Basic needs for anti-virus protection at the Wide Open Corporation

- One of the most important details here is to determine all the network entry/exit points a virus or other malicious code could use. A detailed diagram of these locations must be created if not already available. Protection at all these points must be included in the implementation plan.
- Standard computer entry points are, floppy disk and CD-ROM. The product(s) chosen must have the ability to scan for virus activity on these and any other type of fixed or removable media.
- Other entry/exit points to computers are, network connectivity, email and Internet connectivity.

Implementing the 'multi-vendor' approach at the different tiers
For simplicity, the anti-virus vendors will be referred to as 'vendor1', 'vendor2' and 'vendor3' for the remainder of this document. File or print servers will be referred to as 'Local Servers'.

The key components to the solution are as follows.

- Tier 1: User Computers & Tier 2: Local Servers

  Both user computers and local servers will utilize anti-virus protection for the operating system utilizing vendor 1.
- Tier 3: Email Servers
  Email servers will utilize server anti-virus protection for the operating system utilizing vendor 1, email anti-virus protection utilizing vendor 2 and finally, a 'content-scanner' utilizing vendor 2 or if possible, vendor 3.
- Tier 4: Gateway Servers
  Each of the servers will utilize server anti-virus protection for the operating system utilizing vendor 2 or 3, and a 'content scanner' incorporating one or more anti-virus scanners for various Internet protocols, to include SMTP, HTTP, and FTP utilizing vendor 2 or 3.
  Remember that HTTPS traffic is encrypted and cannot be virus or content scanned until it is opened at its destination.

Anti-virus product support options for the Wide Open Corporation
This section defines the different operating systems, email systems, and other types of data/protocols the anti-virus products must be compatible with. This information will be very important when choosing which anti-virus products to purchase.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Hardware requirements

When selecting the various anti-virus products, it must be established whether the current hardware on desktop and server machines meets with the minimum hardware requirements of these products. This will help to avoid installation issues during the implementation. It will also help to determine if additional servers or hardware upgrades are necessary before the implementation, which could add additional time and cost to the project.

Important Product Features

Following is a list of product features that are important for the implementation, management and maintenance of the solution.

- Automated remote or local product installation/removal
- Automated remote or local removal of other vendor products
- Automated distribution of product updates/upgrades
- Automated retrieval of virus definitions
- Automated or manual definition push and virus scans
- Ability to roll-back defective virus definitions
- Automated Alert Notifications
- Ability to scan compressed or archived files (multiple layers)
- Ability to exclude specific files or folders from scanning
- Multiple actions available for infected files
- Central Quarantine
- Ability to delegate administrative roles in anti-virus product(s)
- Central (including remote) management of product(s)
- Detailed manual or scheduled reporting
- Ability to use two or more scan engines
- Stable and reliable anti-virus engines
- Proven track record of virus detection

Step 2: Evaluate the current company anti-virus policy

Responsible management of an anti-virus solution

It is extremely important that all staff members involved in managing an anti-virus solution should know exactly what their responsibilities are. In order for any anti-virus solution to be truly effective, it should have clearly defined policies and documentation outlining at least the following items:

- Groups responsible for the various components of the solution
- Lead administrators for the various components of the solution
- Point and method of contact in the event of a virus issue
- Procedures to be followed in the event of a virus issue
- Procedures to be followed to determine the source of a virus, and what needs to be changed to eliminate the risk of this type of virus recurring
- Procedures to be followed for maintaining an anti-virus solution
- Central administrator/group for the entire anti-virus solution

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

User Education

Users need to be instructed on company 'best practices' for at least the following.

- Sending/receiving email and attachments
- Browsing and downloading from the Internet
- Handling files on removable media (floppy disk, CD-Rom, etc.)
- Who to contact in the case of a virus alert on their PC.

The best way to deploy this information is through a company-wide anti-virus policy. The policy could be broken down into sections for each of the four items above. Alternatively, a separate policy could be written for each item. Whatever the format, the policy should be clearly defined and easy to read. The policy or policies should then be distributed to all employees.

Step 3: Evaluate the existing anti-virus solution

Evaluate the existing anti-virus solution focusing on maximizing its configuration, or, if necessary, replacing it with a product(s) that more closely fits the company needs as defined in step 1.

In the case of the Wide Open Corporation, it has already been decided that a new product line is required. Since the needs of the company are also defined in step 1, the next step is to research the available anti-virus products on the market.

Step 4: Research the available anti-virus products

Since it has already been determined that a replacement is necessary, you must now lay the groundwork for evaluating the 'best alternatives' on the market.

Where to start

The Internet is the perfect place to find all the product information needed. In the vast majority of cases, a 'trial version' of most products can be downloaded for testing and analysis. Some vendors will actually allow you free access to call their tech support line with questions, even though you are not an actual paying customer.

Links to several anti-virus vendor sites are listed on page 15 under the heading 'Vendor Product Links'.

To assist in selecting products for testing, the creation of a product matrix is recommended. The matrix should include items such as:

- Types of anti-virus coverage required. i.e. Operating System, Email, etc
- Product features required (see 'Important Product Features on page 10)
- Cost of product(s)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The creation of this type of document will make it easier to eliminate products that don't fit the bill, leaving only the products that can be used in your specific environment.

Step 5: Test the product(s)
Once the available products have been narrowed down to a manageable number, these products should if possible, be tested in a 'lab environment'. NOTE: To avoid major issues in a company's production environment, it is strongly recommended that all software testing of any kind be completed in a non-production or 'lab environment'.

Step 6: Create the implementation plan
Once product(s) selection has been accomplished, the creation of a detailed implementation plan is vital to the success of the new product(s). The plan should include all aspects of the implementation including, removal of existing products, deployment of the new products, names of personnel involved in the deployment, and recovery procedures.

Step 7: Implement the product(s)
Implement the new product(s) following the implementation plan created in step 6.

Step 8: Regular review of the anti-virus solution
Once any software implementation is completed, there will always be a need to apply revisions and updates to the product from time to time. Hopefully with the anti-virus product(s) chosen, most of this work can be automated using built-in tools such as a 'central administration console'.

However, there are a couple of important items to keep in mind after implementing an enterprise anti-virus solution.

- As mentioned earlier in this document, anti-virus vendors are constantly updating/enhancing their products to keep pace with the latest virus threats. Some vendors do a better job of keeping up with virus threats than others. There is also the possibility of totally new products coming on the market that more closely match your company's needs. It is therefore recommended that you review your existing anti-virus products from time to time to ensure they are keeping pace with the current virus threat.
- The other change that will certainly occur is change in the size of your company. It will hopefully expand! This will mean more computers to protect and could mean more locations for branch offices in other cities or countries. Even with the best thought out implementation plan, it is not always possible to predict how fast a company may grow and how scalable the anti-virus solution needs to be. Whether the company grows or shrinks, it is also recommended that any review of the existing anti-virus solution should be done keeping in mind the current size of the company, and it's plans for the future.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The reviews mentioned above should happen at least every twelve months, or perhaps after any major change in the structure or size of the company.

Conclusion

Anti-Virus protection is a vital part of any enterprise security plan. Because of the nature of virus activity, it requires a lot of maintenance in order for it to effectively perform its role. If the anti-virus products chosen to protect your enterprise are chosen wisely, the amount of time spent on maintenance can be significantly reduced. This can also reduce the risk of issues due to 'human error' when performing too many manual tasks in the anti-virus configuration.
Implementation of anti-virus products requires a lot of planning. A thorough implementation plan should cover every possible aspect of the project including back-out plans should any issues arise. An enterprise-wide anti-virus policy is a key part of the implementation.

Combining the above items with a policy that covers user training/guidelines, and administrative roles/responsibilities, will help create an environment where all employees assist in defending against today's and tomorrows every increasing virus threat.

References

[1] Internet Security Systems. Schoeniger, Eric. Securing The Internet Economy. Holliston, Mass: Info World. (2001): 27.

[2] British Department of Trade and Industry. Information Security Breaches Survey 2002. UK: British Department of Trade and Industry. (2002): 12. http://www.pwcglobal.com/Extweb/ncsurvres.nsf/0cc1191c627d157d8525650600609c03/845a49566045759e80256b9d003a4773/$FILE/ATT7PG80/DTI Security Survey 2002.pdf (March 20, 2003)

[3] iCSAlabs. "Why is the David Smith (Melissa Author) Prosecution Important?" URL: http://www.icsalabs.com/html/communities/antivirus/melissa/melissa3a.shtml (March 18, 2003)

[4] searchSecurity.com. "Virus" July 30, 2001. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213306,00.html (Feb 25, 2003)

[5] searchSecurity.com. "Worm" April 20, 2001. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213386,00.html (Feb 25, 2003)

[6] searchSecurity.com. "Trojan Horse" May 10, 2001. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

(Feb 25, 2003)

[7] searchSecurity.com. “Hacker” June 12, 2001.
URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212220,00.html
(Feb 25, 2003)

[8] searchSecurity.com. “Cracker” October 14, 1999.
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211852,00.html
(Feb 25, 2003)

[9] searchSecurity.com, Cluley, Graham. “Beating malware: Beyond antivirus software.” October 4, 2001.
URL:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci774046,00.html
(Jan 15, 2003)

Vendor Product Links

Clearswift Limited. “Clearswift MIMEsweeper e-policy products for email and web.” 2003.
URL: http://www.mailsweeper.com/products/msw/default.asp (March 17, 2003)

Command Software. “Product center.”
URL: http://www.commandsoftware.com/products/index.cfm (March 17, 2003)

F-Secure. “Virus Protection and Intrusion Prevention Products.”
URL: http://www.europe.f-secure.com/products/anti-virus/ (March 17, 2003)

GFi Limited. “GFi Security and Messaging Software.” 2003.
URL: http://www.gfi.com/ (Jan 15, 2003)

NetIQ. “Internet Content Security.” 2003.
URL: http://www.mailmarshal.com/ (March 17, 2003)

Network Associates Technology Inc. “Products.” 2003.
URL: http://www.mcafeeb2b.com/products/ (March 17, 2003)

Sybari Software Inc. “Products.” 2002.
URL: http://www.sybari.com/products/ (March 17, 2003)

Sophos. “SOPHOS anti-virus for business.”
URL: http://www.sophos.com/products/software/ (March 17, 2003)

Symantec. “Enterprise Products and Services.” 2003.
URL: http://enterprisesecurity.symantec.com/content/productlink.cfm?EID=0
(March 17, 2003)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Trend Micro. “Products.” 2003.
URL: http://www.trendmicro.com/en/products/global/enterprise.htm
(March 17, 2003)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.