Global Information Assurance Certification Paper

Antivirus Management

From An Outsourcers Perspective

Robert Mackintosh: GIAC GSEC v1.4b
Submitted: 28/05/2004

Introduction.

IT Outsourcing is becoming more and more competitive and the service offerings provided by an outsourcer are becoming more and more complex. Outsourcing companies need to offer their services better than their competitors in order to stay in the game.

Information Security is the fastest growing area in IT today. Companies are putting more money into protecting their assets and Hackers are putting more time in developing tools that are harder to defend against and cause more damage. An outsourcer needs to be in a position and prepared to jump into the IT security game now in order to get some of the market share and Antivirus management is a fundamental service to start with.

There is a plethora of products and tools on the market that are designed to help protect an environment from falling victim to most known forms of Malware, mainly Virus's, Worms, and Trojans. The challenge for the outsourcer is to manage these tools to their full potential whilst being cost effective and cost competitive.

The purpose of this paper is to document the key areas that an outsourcer should focus on when setting up Antivirus Management as a service offering. It is also intended to point out some of the key configurations that should be considered when configuring Antivirus software. The document starts from the top with some ideas around constructing and documenting a Service Description moving all the way through to technical configurations.

Key & Definitions

Term	Description
Pattern File	Also known as DAT file, Definition file, Signature File. The term Pattern file is used by Trend Micro: http://www.antivirus.com
Malware *	*Malware – short for malicious software – refers to any malicious or unexpected program or code such as viruses, Trojans, and droppers. Not all malicious programs or codes are viruses. Viruses, however, occupy a majority of all known malware to date including worms. The other major types of malware are Trojans, droppers, and kits. Due to the many facets of malicious code or a malicious program, referring to it as malware helps to avoid confusion. For example, a virus that

	also has Trojan-like capabilities can be called malware.
Trojan *	*A Trojan is malware that performs unexpected or unauthorized, often malicious, actions. The main difference between a Trojan and a virus is the inability to replicate. Trojans cause damage, unexpected system behavior, and compromise the security of systems, but do not replicate. If it replicates, then it should be classified as a virus. A Trojan, coined from Greek mythology's Trojan horse, typically comes in good packaging but has some hidden malicious intent within its code. When a Trojan is executed users will likely experience unwanted system problems in operation, and sometimes loss of valuable data.
Virus *	*A computer virus is a program – a piece of executable code – that has the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of file and are spread as files that are copied and sent from individual to individual. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. If the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer. Several years ago most viruses spread primarily via floppy disk, but the Internet has introduced new virus distribution mechanisms. With email

	now used as an essential business communication tool, viruses are spreading faster than ever. Viruses attached to email messages can infect an entire enterprise in a matter of minutes, costing companies millions of dollars annually in lost productivity and clean-up expenses. Viruses won't go away anytime soon: More than 60,000 have been identified, and 400 new ones are created every month, according to the International Computer Security Association (ICSA). With numbers like this, it's safe to say that most organizations will regularly encounter virus outbreaks. No one who uses computers is immune to viruses.
Worm *	*A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or email attachments.

*Terms provided by Trend Micro;
http://www.trendmicro.com/en/security/general/glossary/overview.htm

Note: When the word virus is used it is intend that it is used in its generic term covering most common forms of Malware such as worms, Trojans, and viruses, unless otherwise stated.

Service Description

As with any service offered by an outsourcer it is critical that a service description is documented for each service offered to a customer. Without a service description it is impossible to standardise the activities carried out for all customers, as each customer could have been sold a different service.

The sales team would use the service description for Antivirus when they are selling the service to a new or current customer. The service description lists all the aspects of the service that the outsourcer can offer and ensures that nothing is sold that can't be delivered. It is not uncommon for a sales or bid team to offer something that the delivery teams can not provide, the underlying cause of this is usually the lack of a service description.

As well as aiding the Sales team in selling a service correctly, a service description is required by the team that provides the service after the sale has been made. As part of running an outsourcing organization it is important to know what the cost of delivering a particular service is, including the number of headcount required to deliver that service. For example, an organization may calculate that one staff member can support thirty Windows servers that conform to a standard operating environment (SOE). Ensuring that a service description is in place makes the job of calculating the number of headcount required to support a customer easier because there should be no surprises as to what service the delivery team needs to provide.

It is not uncommon for an Antivirus service description to be incorporated into a larger Security service description as many organizations recognize Antivirus as a component of an overall Security service, especially if they follow methodologies such as ITSM. No matter how the service is presented it is important to list the key components of the Antivirus service. Some are listed below.

- Regular definition file updates.
- Monthly Report listing
    - Malicious code detected in the environment.
    - How an infection penetrated the environment.
- A notification of new medium/high level virus's detected in the wild. E.g. As reported by an Antivirus vendor.
- Definition file update and distribution tracking.
- Outbreak management and clean up.
- Technical information and guidance for non-managed (not managed by the outsourcer) node or networks.
- Operating System security patches will be installed on a regular basis.

It is also important to document caveats to the deliverable components of the service. Some examples are listed below.

- Monthly Reporting – A management console is required that supports report generation and each requested item of the report must be supported by the report generation tool.
- Regular definition file updates – The software license with the Antivirus vendor must be current.

Once a service description is in place it should be clearer to all parties as to what the service entails. The sales team knows what they can sell a customer, the customer knows what to expect from the outsourcer, and the support technician or group knows exactly what is required of them when delivering the service.

Roles and Responsibilities Matrix

With an outsourced Antivirus service it is near impossible for the outsourcer to take responsibility of every aspect of the service. For example, it is impossible for the outsourcer to manage the antivirus software installed on a laptop if that laptop never connects to the network. All that the outsourcer can do is ensure that there is a mechanism in place to ensure the laptop receives the updated pattern file when it does connect to the network.

Another area the outsourcer most probably would not have any control is around User Management. User Management includes tasks such as policy enforcement (that requires HR involvement) and training. The outsourcer may supply training material to the customer but it is up to the customer to ensure all their staff are trained in their role of Antivirus Management.

It is not uncommon in an outsource agreement for an organization to outsource the support of only some of its systems or network. This could create a situation where, if not documented, the roles and responsibilities of antivirus management on non-outsourced systems could be unclear. For example, the customer may be responsible for the installation and maintenance of antivirus software on the server itself but the outsourcer may be responsible for making the updated definition files available on a distribution point. Unless it is documented this process would probably break down and the server may never be updated.

Below is an example Roles and Responsibilities matrix.

Virus Protection	Outsourcer	Customer
Monitoring of servers for virus infections on outsourced systems	x	
Update virus definition files as published	x	
Update virus definition files when a major outbreak is identified	x	
Rectification of virus infections on outsourced systems	x	
Where possible, ensure protection software is running continuously on all distributed systems and advise *customer* of any instances where this is not possible	x	
Ensure anti-virus software on desktops and laptops is not disabled, to the extent that the ability for the user to disable the software is controllable	x	x
Prepare the internal anti-virus systems policy		x
Approve or reject the internal anti-virus systems policy		x

Virus Protection	Outsourcer	Customer
Where the source of a virus is identified as a business partner of *customer*, notify the business partner of the virus infection and follow up on steps taken to rectify		x
If an infection is found, isolate the infection in accordance with agreed policies	x	
Report on major viruses outbreaks, detailing actions taken to resolve and prevent recurrence	x	
Use reasonable efforts to ensure that Desktop PC users do not disable anti-virus tools		x
Use reasonable efforts to ensure that end users do not connect devices without current anti-virus tools to the *customer* IT Environment		x
Scan all disks prior to insertion into *customer* PC's		x
The *customer* Security Policy must include provisions for Virus Protection at the Email, Server, desktop & notebook levels including automatic monitoring for viruses and automatic repair or deletion of infected files.	x	x
Customer must maintain a subscription / maintenance service for all anti-virus software that it uses for virus protection, which provides for regular scan file updates and assistance i.e. support for instances where vendor support is required.	x	x

As can be seen from the table above there are some items where the outsourcer is responsible and others where the customer is responsible, there are also items that have joint responsibility. No matter what the item, it is important to document who owns the responsibility of an item to ensure that each party knows their roles and responsibilities.

Antivirus Policies.

An Antivirus policy is key to any antivirus infrastructure and is the foundation on which the antivirus processes are developed. The Antivirus policy contains the detailed information on what each tier of the Antivirus infrastructure is to achieve. Without this information it is near impossible to create the processes for Antivirus management. The policy ties all the tiers together at a high level to achieve a Defence in Depth. An Antivirus policy is also necessary to ensure that every person that connects to the environment knows the role they play in Antivirus management. For a good reference to Security policies *The CISSP Prep Guide (Gold Edition) by Krutz, Ronald L & Vines, Russell Dean, pages 11 to 15* is a good reference.

As an outsourcer, it is important to remember that there is a large possibility the customer you are about to support has very little idea when it comes to Security and Antivirus Management. Due to this lack of knowledge you may also find that they do not have an antivirus policy and would not know how to create one if it was suggested to them.

Having an Antivirus policy template is a very useful tool when introducing an Antivirus service into a customer. Although an antivirus policy may differ from customer to customer there are still some fundamental requirements to ensuring a solid antivirus service. Having an antivirus policy template that can be used on multiple customers with very little modification helps an outsourcer to standardise the processes used across all those customers. In the end this standardisation reduces the cost of delivering a service.

It is never good when a virus infection or outbreak occurs in the environment due to a user not following policy, for example opening an email attachment from somebody they do not know when the antivirus policy specifically states not to do this. It is even worse when a support staff member makes the same mistake. By having a policy standardised as much as possible across all customers there is less chance for a support staff member to contravene the policy because the actions they take on each customer will be the same.

An organization may require an antivirus policy for different areas of the organization. One antivirus policy that suits this category would be a policy for the user base. This policy is intended to ensure that every user that operates on the network knows what is required of them in protecting the infrastructure from malicious code.

No matter if there is a single policy that covers all tiers of an environment or if there is a policy for each tier, an Antivirus policy is a key document required when ensuring the protection against malicious code. Without a policy it is unclear what is to be achieved and hence processes can't be written.

Standard Operating Environment (SOE)

Imagine knowing exactly what you manage before a server or workstation is even put on the network. This is the point of a Standard Operating Environment (SOE). An SOE build is a complete environment that has been tested both for stability and useability and is the baseline for the server or desktop type it is intended. For example the SOE build for a Windows IIS server could be a Windows 2000 Operating System with IIS installed. IIS could be configured to have various security settings such as the default website disabled. The Operating System would have the latest security patches applied up until a certain date, the Guest account would probably be removed, and the Administrator account would be renamed, and this is just to list a few. The *MCSE Windows 2000 Professional Exam Cram Chapter 2, by Balter, Dan & Holme, Dan & Logan, Tod & Salmon, Laurie* is a good reference for overall Windows 2000 Workstation security settings.

No matter what configurations have been made with the SOE, the point is that you, as the Antivirus administrator, will know exactly what you manage. As an example, the worm WORM_NETSKY.R (Trend Micro –www.antivirus.com) exploits a vulnerability within Internet Explorer. This vulnerability is corrected with the application of Microsoft patch MS01-020 (http://www.microsoft.com/technet/security/bulletin/MS01-020.mspx). Knowing that the SOE for all workstations and servers has had the MS01-020 patch applied lets you know that the impact the worm will have on the environments you are managing will be minimal. This allows you to focus on proactive tasks such as pushing out pattern files and watching the network for suspect traffic rather then the reactive process of frantically trying to patch all servers and workstations with the security patch.

An SOE also ensures that antivirus software is installed on every new computer that is put on the network and that it is configured correctly. In basic terms, an SOE image is made by running up a computer with the operating system, required applications, Service Packs, hot fixes, security configurations, application settings, and any other setting that are required to ensure the functionality of the system. Once tested, an image of the installation is made using imaging software. The image is then put onto a media that is available to the technicians to install.

The baseline for any node should be recorded in a Configuration Management Database.

Configuration Management Database (CMDB)

A Configuration Management Database is a database that contains details of all the elements (e.g. a server) within an organization's IT infrastructure. Each piece of information within a CMDB is called a Configuration Item (CI). All the CI's would come together to record the baseline of an element. To ensure that all changes to a CI or the addition of a new CI is recorded a CMDB should be integrated with a Change Management system. A good reference to IT Service Management (ITSM) and Configuration Management is http://www.itil-itsm-world.com/. From this page you should brows to "Configuration Management" to read about the methodologies around a CMDB http://www.itil-itsm-world.com/itil-1.htm.

A CMDB could contain simple configuration items such as:

- Details of the system owner
- The IP Address of the server
- Hardware type
- Hours of support
- Location of the node
- Security classification e.g. Internet facing
- Reference to the documentation store

- Installed Security Patches

All these entries in the database would be relevant to an outsourcer in the day-to-day support of a node. With Antivirus administration it is critical to know what services are running on a machine. For example, CodeRed attacked a vulnerability in Microsoft IIS that gave system level privileges to a remote attacker. The best way to protect against Code Red is to apply the Microsoft vulnerability patch MS01-033 (http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx) that closes the vulnerability in the Indexing server. Knowing exactly which servers have IIS installed will cut down the time it would take to get the environment or environments you administer protected.

CodeRed Example

As an example of the impact the lack of a CMDB can have on a support infrastructure we will take the CodeRed scenario. Let's say you look after twenty customers and all their Windows servers combined add up to five thousand, out of the five thousand ten percent are running IIS, so that is five hundred. Without a CMDB you would have to scan all twenty customers or, more to the point, all five thousand servers to determine which are running the IIS service. This could take days and you have not even got the patch deployed. Within that audit period there is a good chance that a large percentage of the servers running IIS would be infected. On top of the audit process there are some other tasks you need to complete such as testing the patch and organising outage windows to apply the patch, and then you need to install the patch to all five hundred servers. Considering that within about a week of being detected CodeRed had infected hundreds of thousands of servers running IIS there is a good chance that a large majority of the IIS servers out of the five hundred would have been infected. Now think of the cleanup costs.

Now let's take the example where a fully maintained CMDB is in place. The vulnerability is announced and Microsoft releases the patch. As part of the risk assessment process you query the CMDB for all servers running IIS. Within a matter of minutes you know that there are five hundred servers that are vulnerable. You also know the name, IP Address, location, system owner, security rating, and any other bits of information you may need to prepare and install the vulnerability patch. Because of this information you quickly come to the conclusion that the deployment of the patch is critical and you can then streamline your testing of the patch to suit. Once the testing is completed the Change Management process is done and now the patch can be deployed inline with the outage schedule. There is one final step that is done and that is to record the change made to the systems back into the CMDB. The updating of the CMDB ensures that if the server is rebuilt it is restored to the correct baseline; this baseline now includes the CodeRed patch and ensures that the server will always be protected from CodeRed, even if it is rebuilt.

Comparing the two scenarios shows the definite advantages of having a maintained Configuration Management Database in place. For one, the audit

process is much faster with a CMDB, with a CMDB the audit takes minutes but without it could take days. Because with a CMDB you already know which servers are running IIS you can raise the Change Requests in parallel with your testing, this again speeds up your preparation time. Without a CMDB you don't know which servers are running IIS until you have completed the audit so how can you raise the Change Request? Once the patch is installed on a server this change is then recorded in the CMDB and the baseline of a server is updated. This recording allows you to go back at the end of the patch rollout and determine if any servers were missed. It also allows you to restore a server to the correct baseline should it need to be rebuilt. Without the CMDB you would have no reliable or manageable way of recording this change.

The purpose of a configuration management database is to store all the information about the environment the customer is paying you to manage. Without a CMDB it is near impossible for an outsourcer to know what it is managing and hence to do it's job effectively.

Antivirus Management Procedures and Implementation

An outsourcer needs to take two things into consideration when putting in place a new antivirus solution or setting up management procedures for an existing implementation.

When implementing or managing an antivirus infrastructure you want to put the best possible solution in place. A tiered approach is the best way to ensure that every layer of the infrastructure is protected and that there are multiple points that a virus can be detected and removed. You also need to look at the solution from a manageability point of view, after all the easier an antivirus solution is to manage the more cost effective it is to support.

There are a number of theories when it comes to implementing an antivirus infrastructure. One common practice is to use a different antivirus vendor for each tier of the network. From a Defence in Depth perspective this is seen to be good practice because at the time of a new virus or worm being detected in the wild it is not uncommon for one antivirus vendor to be ahead of the others in releasing a pattern file. Of course, it is not always the same vendor who is first. Very occasionally a vendor has actually released a pattern file that breaks the antivirus software and this is not corrected until an updated pattern file is released, this can render a tier of protection useless. In either scenario, by having multiple vendors protecting the environment there is an increase in confidence that at least one tier of the network is protected.

The problem with having various products in an environment, as opposed to one, is that the administrative load increases. Rather than having one management console to monitor you may have multiple. There are also multiple processes that have to be followed when updating pattern files, etc. Combine this with supporting multiple customers and suddenly antivirus

management is an expensive task and, of course, this is not taking into account managing and cleaning up an outbreak situation.

No matter which theory is followed there are some key tiers that need to be considered - the Management tier, the Gateway tier, the Email tier, the Sever tier and the Desktop tier.

The Management Tier.

The first tier is the Management tier. From this tier the entire antivirus infrastructure is managed, updates can be controlled, reports can be run, outbreak tracking and infections are visible, etc. This is also the tier that makes antivirus management cost effective and efficient from an outsourcer's point of view.

With a good management solution in place one antivirus specialist can support many servers and possibly customers. A good solution will allow all the tiers of the network to be managed from one central point and allows automation of the tasks the antivirus specialist needs to perform. For example, it should support a schedular that automates pattern file updates. It can be configured to download pattern files from the vendor at a specific time or interval and then deploy them to the clients at a set time or interval. This type of configuration is important as it removes human interaction from the process and frees up the antivirus specialist to do other tasks. The report generation capability of the management software is also very important, this is the report that is presented to the customer and management every week or month or whenever scheduled, reporting is discussed later in this paper.

The Gateway Tier

From an Internet perspective the most common vector for a virus or worm to enter the network is via email (SMTP) followed by http traffic. Fortunately there is a plethora of solutions available for you to choose from. There is SMTP gateway software available for most operating system types, e.g. Windows and Solaris, and there are different reasons for choosing each. When choosing a solution you should keep in mind not only the technical requirements of the solution but also the support requirements. For example, if you, as the outsourcer, are predominantly a Solaris house it would be unwise to implement a Windows solution as the training and hiring of staff to support the new solution would probably be too expensive to justify the choice. You could also be introducing single points of failure.

Most SMTP gateway products offer an antivirus service as well as a SPAM management service. These two services go very well together as it is not uncommon for a worm to generate email that a SPAM management service

can detect as SPAM, and consequently it is not uncommon for SPAM mail to contain a virus. Having both services on a gateway makes this tier more effective in stopping malicious code entering the environment.

Security patching of any gateway server is critical due to their proximity to the Internet. The last thing you want is for a hacker to disable Antivirus services through a vulnerability that is closed by a specific security patch. If this were to happen you would loose the first line of defence against virus's entering the environment you manage. Many vulnerabilities give an attacker administrative access to a server and by not applying security patches could give the attacker access to confidential email that pass through the email gateway.

The Internal Email System

The next tier down from the gateway tier is the internal email system. Running an antivirus service on the internal email system is critical as email is the most common vector for the spreading of virus's and worms on an internal network. For example, at the time of writing this paper the Netsky worm was causing the most damage to organizations; see below for a description of the W32.Netsky.W worm provided by Symantec (http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.w@mm.html).

"W32.Netsky.W@mm is a minor variant of W32.Netsky.N@mm. This variant is also a mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives.

The "sender" of the email is spoofed, and its subject, message body, and attachment vary. The attachment has .exe, .pif, or .scr as extension. The worm may also send its zipped copy as attachment.

This threat is compressed with UPX"

As this is an email bound worm there is a definite requirement to scan all email moving through an organization.

There can be quite some time between when a virus or worm is released into the wild and when an antivirus vendor has a pattern file that can deal with the new threat. There is also some time from when the pattern file is released and all the systems you manage receive the pattern file. This window of time is when the systems you manage are most at risk. The internal email system is usually the first service to be impacted in this time. This is not good as it can be the main vector for the virus or worm spreading to other systems.

Having antivirus detection running on the internal email systems will, once a pattern file is released and installed, detect malicious code that got through the gateway detection and should remove it. This detection will also aid in

tracking the source of an infection on the network. For example, you will be able to track down the mailbox that is distributing infected email to other parts of the organization and remove the infection.

Another point to remember when implementing antivirus software on email servers is to ensure that the operating system is protected. Most antivirus vendors will have a separate product for scanning and cleaning email but this product will not protect the operating system itself so it is important to install the software intended for this task. You will also need to configure the operating system scanner to ignore some files and directories, or possibly an entire partition or physical drive. One of these exceptions would be the Message Store in Microsoft Exchange. You would not scan this location as it is scanned by the email scanner and the file system scanner may corrupt the information.

File and Print Servers, Plus Others.

This category covers all the servers outside of the gateways and internal email servers discussed above. Some example servers would be, file servers, print servers, domain controllers, and database hosts. This is also the tier that hosts a company's most critical data and hence requires protection.

When configuring antivirus software on a server in this category there are some things you need to take into consideration such as:

- When should a scheduled scan run
- What is the impact of Real Time Scanning and should it be on
- What files, file types, directories, or drives should be excluded from a scan?
- How should infected files be handled?

A scheduled scan is critical to ensure that a server is free of infection or infectious files. Even though Real Time scanning will detect malicious code entering or leaving the server it will only detect code known by the pattern file. If a new worm was to be copied to the server and this new worm was not know by the pattern file then it could successfully be copied and possibly infect the server. Once the file is on the server Real Time scanning will not be effective on this file until it is accessed. A scheduled scan ensures that all files (minus those in the exception list) are scanned with the latest pattern file and will detect any malicious code that made it past the Real Time scanner.

Real Time scanning is one of the most effective processes for preventing a system from sending or receiving known malicious code. When a file is accessed the real time scanner will check the file for known virus signatures and, if a file is found to be infected it will take action before the file reaches its destination. Real Time scanning can also impact server performance. If a server processes many file transfers or file modifications there may be a business decision made to disable Real Time scanning due to the server

being unusable because of slow performance. In this situation a schedule should be put in place to allow for more frequent full system scans to be run to make sure that infected files are detected and processed.

An alternative to disabling Real Time scanning is to put exclusions on certain file or mime types or excluding certain directories from being scanned. A common example of this is to exclude database files from a scan. This will reduce the impact that scanning has on a system because trusted files are not scanned but all other files will be scanned, thus reducing the chance of infection from the majority of file types.

It is not uncommon for a critical or business related file to be infected with a virus and if this does occur you may not want to delete the file, especially if it has not been backed up. In order to have the ability to try and clean the file manually you may want to configure the antivirus software to first try and clean the file and then, as a backup, if the file can't be cleaned you may want to quarantine it rather than delete it. On the other hand the antivirus policy may state that if a file cannot be cleaned then it is to be deleted.

The Desktop Tier.

The Desktop environment is by far the hardest tier to manage and the main reason for this is that there are usually a large number of clients. The fact that there is a person sitting behind the keyboard of every desktop is the main reason why the desktop is the most at risk.

The configuration of an antivirus desktop client should require as little input from the user as possible. There are also some things you will want to prevent the user from doing. Some examples of controls you would want to remove from the user are:

- Ability to disable the antivirus service
- Ability to disable or cancel a scheduled scan
- Ability to disable Real Time Scanning.

Some of these items are configured when the SOE is built and others are configured from the management console. This will depend on the product.

When configuring the desktop scheduled scan time, it is important to remember that when a scheduled scan is running there will be considerable performance impact to the machine. Because of the impact to performance most users, due to their lack of knowledge, will attempt to stop the scan. To minimise the impact that scanning will have on the users productivity you should look at running the scan when it is going to least impact the user, this would usually be at night when the user is not at work. One problem with running a scan at night, or outside of business hours, is that a lot of users will shut their machine down and hence it will not get scanned, or, due to the smarts in the software it will get scanned when the machine is next turned on.

One of the worst times for a scan to run is when the user first logs on because this is the time that they are ready to work. A good time to run a scan is at the user's break time; let's say Thursday at 12:00pm. With the user knowing that this is the scan time they can plan to go to lunch whilst the scan is running and when they get back they will be able to use the full performance of their machine. Whatever time the scan is set to run, it is important to minimise the impact to productivity.

Another tool that you will want to consider is user alerting. Alerting through the management console was talked about previously but you may also want to activate user notifications through the antivirus client software as a user contacting the Service Desk can be one of the most effective ways for getting an infection removed from the network. Most products will alert the user of a virus through a pop-up window on the screen and will inform the user of the file that has triggered the alert and the action that was taken. Most notifications can be customised with details such as the Service Desk number that will give the user more instruction on the actions to take.

Some form of user training is always a good idea and, as an outsourcer, you should encourage your customers to train their staff in the basics of how the antivirus software works. For example, it is helpful for a user to know if the antivirus software has failed to start after a reboot. Most vendors use a visual notification indicating that there is a problem with the software. On a Windows system the icon in the Task Bar may change colour, change icon, or not appear at all. These are very easy indicators for a user to monitor and should they notice an error they should contact their support service. This information and process is easy to publish and could be displayed on an intranet web page.

Some Good Practices

Regular pattern file updates are critical in the protection of the environment you manage. As a good practice you should try and ensure that there is more than one way a machine can receive new pattern files. For example, many antivirus clients can be set to download their pattern files independently from the vendor site as a backup to getting them from the management distribution point. This kind of backup is effective but it can cause an impact to the network in low bandwidth situations where normally the pattern file would be distributed outside of business hours. As this would only be a backup and pattern files would usually get updated in a controlled manner off the managed distribution point, a business decision could be made to accept occasional network impact to ensure the antivirus software is up to date.

Another good practice is to record when an antivirus update occurred. This is useful information when generating a report for the customer as well as tracking the proof that you are doing your job. By recording the time and date that you distributed the pattern file you can show that you are meeting (if one

is set) the SLA that states you will distribute a pattern file within a certain time of the vendor releasing the file.

Regular auditing of the antivirus infrastructure is a good idea. It is very easy when managing possibly thousands of servers and tens of thousands of desktops to miss seeing machines that are failing to update or where the software has stopped working. It is also not uncommon for servers or workstations to be put onto the network without antivirus software. Regular auditing will help remove these risks from the network. You should scan the network for machines without antivirus software; most vendors have a tool for doing this. You should also work through the management consoles and correct any machines that are not up to date. It can be a good idea to have a different person to the normal antivirus administrator run the audit so that there is a new set of eyes viewing the infrastructure.

Sophos Antivirus offers a good reference to best practice at http://www.sophos.com/virusinfo/bestpractice/

Standardisation

When managing multiple customers, standardisation is the key to being cost effective. Standardisation also ensures a better service as there is less chance for mistakes.

In a perfect world you would have all your customers on the same antivirus product but of course this does not happen. Most products perform roughly the same so there is a lot of opportunity to standardise the tasks required for antivirus management. You should try and standardise tasks such as the update time, reporting time, layout of the management console, infection reporting notifications, etc. A good document to have on hand is a document outlining your preferred antivirus product. You should list out the advantages that you see this product has over others so that a customer can see your reasons.

Communication

Antivirus management, like a lot of other security practices, is invisible to the organization when it is done properly. Being invisible can have its disadvantages as management can forget that the job is being performed. As an outsourcer you want to show that you are doing your job to the customer. You should generate regular reports and publish these back to the customer so that they can see the role you are playing in protecting their data. This is especially useful around contract renewal time. Report generation can be

quite time consuming but most products have some kind of report generating tool that should cut down on the task. Even if it takes some time to produce the report, remember visibility is the key.

Conclusion

So, as you can see there is more to offering an Antivirus service than just updating pattern files. If you take into consideration and implement the tools and configurations discussed in this document you will be on the right track to providing a cost effective service that also delivers a high standard of protection to your customers.

Documentation is the key to ensuring that all parties involved in the management of an Antivirus infrastructure know exactly what they are responsible for. By spending the time to ensure that all your documentation from the Service Description all the way down to detailed processes are in place you will save time and money in the long run. Every customer, organisation, network, or individual computer is potentially different, but if you ensure that you have generic documentation that can cover the majority of scenarios you will reduce the cost of delivering an Antivirus Management Service.

References

Internet Sources

Trend Micro Inc.
http://www.trendmicro.com/en/security/general/glossary/overview.htm

Microsoft TechNet. http://www.microsoft.com/technet/security/default.mspx

ITIL & ITSM Directory. http://www.itil-itsm-world.com/itil-1.htm

Symantec Corporation.
http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.w@mm.html

Sophos Plc. http://www.sophos.com/virusinfo/bestpractice/

RMAS: Best Practices. http://vpf-web.harvard.edu/rmas/best_practices.html#infosys_4

Books

Krutz, Ronald L & Vines, Russell Dean. The CISSP Prep Guide (Gold Edition). Indianapolis, Indiana:Wiley Publishing, INC, 2003. Page 11 to 15

Balter, Dan & Holme, Dan & Logan, Tod & Salmon, Laurie. MCSE Windows 2000 Professional Exam Cram. Scottsdale Arazon, The Coriolis Group, 2000. Chapter 2

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event