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

Mark de Rijk, GSEC version 1.4b

Sans Amsterdam Nov. 2002

Case study: Implementing Trend Micro antivirus solutions in the enterprise.

© SANS Institute 2003, Author retains full rights.

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

Mark de Rijk, GSEC version 1.4b

Sans Amsterdam Nov. 2002

Case study: Implementing Trend Micro antivirus solutions in the enterprise.

Abstract:

This paper will detail a process a European enterprise firm went through evaluating its current anti virus protection level and how the firm choose to up rate the solution to a defense in depth style installation.
This can be used as a guideline for your own av-solution selection process in your enterprise.

This paper details how we evaluated the current av protection in place, what risks we suffered because of the vulnerabilities in the used products at that time. Also the features in the products in use at that time are discussed. I also will detail why other features have become required for us over time. What we did to upgrade the av infrastructure and to what level of protection will also be detailed by me. This paper also shows you what the results are of upgrading the av protection level. It will hopefully give you pointers on what to look for in av products and what issues can arise when you are deploying such a project.

Before:

At the moment of evaluating the firm's anti virus protection level it consisted it of an uncoordinated decentralized 3 tier solutions.

Before choosing the trend micro solutions, the protection level consisted of a groupware, server and desktop virus scanning solution. While evaluating the current solution several weak points were discovered.

Weakpoints

- Latency in protection availability
- Deployment issues
- No central logging
- Decentralized av policy
- Lack of outbreak management
- Lack of product integration, too much differentiation.

Latency in protection availability

The pattern updates weren't made that quickly available as was desired with all the fast outbreaks of new viruses. We suffered several incidents as some suppliers of which we used the av protection released a patternfile up to 2 days later. This meant in short that before we even had received an update we were left vulnerable for up to 2 days.

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

This meant a huge risk for the enterprise. And every security administrator knows how much a virus incident can cost in revenue losses and so on. This had to be eradicated with the new solution.

Deployment issues

Deployment was also an issue. For instance the pattern updates on the fileservers had to be done manually by installing it by floppy. This created extra time in which a virus could strike.
The timegap in which a vulnerability in the av protection was open could rise up to 8-12 hours. The risk was in that the centrally stored files could be corrupted by new viruses that would reach the fileservers in that timegap.

No central logging

Central logging also wasn't possible as the individual products themselves were not connected to a central management server. This would make it hard to provide a consistent report on the whole av protection infrastructure. At times that would mean I would be creating my own report. This proved to be too time consuming.

Decentralized av policy

Also the issue was that in the case of a border crossing virus incident the blame was put forward from one party to another. Because there were different solutions used throughout the enterprise the detection rate would also vary from one product to another. This would cause for situations where a company would even deny responsibility for infecting a company's network by just saying, you take care of your network and I'll take care of mine. This proved not to be so much of a software issue but more a policy issue.

The above incident had to be ruled out as well to prevent a situation where one company counts on the other company to take care of their anti virus protection.

No outbreak management

Another issue was the lack of outbreak management in the av products in use at that time. This proved to be a small but important issue as there were moments in the company's history where the company suffered some losses in productivity as some returning virus incidents weren't identified as outbreak for the lack of identification of this in the different products in use.
Also because of the sheer volume of detected viruses in such a short timespan as with an outbreak, situations would arise were av products stopped all together and just would let viruses through or stop the entire production process because of the sheer workload.

Product differentiation

The company had offices throughout 15 European countries with autonomous board of directors and it personnel in the different locations. This led to 7 different av protection suppliers.

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

That number had to be brought back to one supplier in order to keep up with the rising maintenance involved in these products.

Because of the different products in use a situation could arise where one product in use at one company didn't detect the same viruses as an av product at the other company as the scanning options and efficiency of the products differed. Centralized and one supplier was the way to go for us

This led to a start for a project group to research how we could take the protection level, raise it and keep down or even reduce the overall cost used for maintenance on the different products.

During:

Before starting this project I looked constantly for ways to improve the av protection level.
About half a year before the start of this project the central management console became a familiarity when looking at the various suppliers. This eventually proved on of the success factors implementing this project.

When selecting the solution to go with there were 2 other suppliers besides Trend Micro which caught our attention. This was the CA anti virus solution and the Symantec solution. Both also had a strong management interface but Trend Micro NeatSuite proved to be the package for us in tests and based on the specs.

So out of this evaluation came the following criteria which a product had to adhere to if possible. For the criteria we chose as our top priority criteria we referenced a document of av protection criteria defined by information security professionals. When discussing the criteria I will detail why we chose to implement the Trend Micro solution and not one of the other 2 solutions.

Selection criteria:

The antivirus solution had to answer to the following criteria if possible all criteria.

- Central administration utility for updating, overview and logging etc.
- Possibility to divide the infrastructure while yet preserving the central administration perspective.
- Scalability is essential; we wanted solutions that work just as well with 20000 users as they do with 20 users.
- Multi platform, not just a fileserver or groupware solution but a suite of tools (remember defense in depth decreases your vulnerability)
- Outbreak management, detection and notification and eradication of a virus outbreak.
- Cost reduction in licensing.

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

Central administration:

Trend Micro NeatSuite features a central management interface for management, logging and configuration purposes.

We wanted a solution where the administration could be centralized while keeping the structure open, scalable and multi platform. The Trend Micro NeatSuite provided us with that as we got a central administrated and updating solution.
All the antivirus products had to be able to be administrated from a central solution if possible. Currently it is far easier to do this but at the time we researched the different solutions only Trend Micro provided us with the most complete package for our specific needs.

Divided infrastructure but centralized.

The product could also be divided and spread across the enterprise while still keeping the centralized management while still being able to offer local administration possibilities throughout the enterprise. What this means is that you can manage a product from the top management interface but also on the product itself (e.g. Officescan).
The 2 other solutions from Symantec and CA provided the central administration but you weren't able to completely manage an individual product from the central management console.

Scalability and limits:

The Trend Micro solutions itself is extremely scalable to organizations with 100000's of computers and so. But there are some limits built into the products of Trend Micro which you have to take in account. For instance with the server protect solution, one information server (central node) is limited to a 1000 servers. While this limit may seem high for the average organization it is a limit which has to be taken into account if you are considering implementing Trend Micro solutions in your company.
Also when deploying Trend Micro NeatSuite across the enterprise, keep in mind that bandwidth will be needed in order for the suite to function correctly.
For the other solutions from Symantec and CA there were no known limits announced for the products offered at that time. But because of the other strong points and the irrelevance of the 1000 server limit for our enterprise this wasn't considered a negative for us.

As we considered scalability one of the priorities we opted to go for a solution where the solution is build on location nodes. As the Serverprotect is build on central information servers as well as Officescan is also build on nodes it is quite easily possible to divide the protection into layers of administration while still keeping a centralized system. This was also quite nicely implemented in the 2 other solutions with a superseding management suite on top and management possibilities for the individual solutions but not quite as in depth as the Trend Micro solutions.

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

Multiplatform / Defense in Depth

The multiplatform and multi OS selection criteria was also well addressed in the Trend Micro NeatSuite as av protection was available for fileserver/groupware/desktop and gateway protection and multi OS wasn't a problem as well as the OS platforms available at that time covered Novell Netware, Windows NT/2000,Solaris HPUX and many more. If you want a complete spec of the different platforms and on which operating systems they are available I invite you to check the Trend Micro website. This proved to be a big plus for Trend Micro. Every platform we used could be protected by Trend Micro solutions. The CA and Symantec solutions varied in cover of the various operating systems and applications but overall Trend Micro was the clear winner there.

The firm opted to go for an expanded defense in depth strategy as we moved from a three tier anti virus protection on the fileservers and the workstations to a true defense in depth solution on the antivirus level. We choose to implement scanning at the gateway level, groupware, desktop and file/application server level. This complemented our perimeter protection of various firewalls and subnetted systems and networks. This created internal perimeters for a virus to penetrate. This would decrease our risk profile because we decreased our vulnerability to viruses.

Because of the multi platform/ multi os solutions from trend micro this could be easily done. This was also possible with the 2 other products but because the operating systems they were available on were limited it was still a winner for Trend Micro. Part of the defense in depth was also the ability to be notified when a component fails to protect. This was also covered at depth by alerts available in number of ways in the Trend Micro solutions. This was also possible with the CA and Symantec solutions but the notification options in those products were significantly less as comprehensive as they are in the Trend Micro solutions.

Outbreak management

Outbreak management was also one of the criteria on our list, while the criterion was of a small priority it was included on the "wish" list. While not necessary at the time of selection it was selected because we released that over time it would become imminent that with the latest destructive viruses it would mean that when pattern file recognition would be unavailable we would have to fall back on outbreak management and prevention. All three products still had there outbreak management and prevention in development at that time. No plus or minus for any of the products evaluated here on this point.

Cost reduction:

A cost reduction was also welcome as some of the products in use were quite expensive in use. Because of a licensing structure based on users the overall cost went down significantly. The price for some products went up but overall a big reduction was gained. If you want to convince management this can be a big plus to get the investment through the board of directors and get it approved. Because of the significant reduction in costs and the number of features required implemented in the Trend Micro solutions the other 2 solutions weren't researched as at that stage Trend

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

Micro came out on top and cost reduction was considered a small factor but not one of priority. Should you wish to research this you can contact your Symantec or CA reseller.

The NeatSuite package at that time consisted of the following products:

- Trend Micro Virus Control System (TVCS) (now Control Manager/ TMCM)
- Trend Micro Officescan Corporate Edition (OSCE)
- Trend Micro Serverprotect for NT/Netware
- Trend Micro Scanmail for Lotus Notes/Domino
- Trend Micro Interscan Viruswall for NT

After choosing to go with the Trend Micro Neatsuite solution we had to make a plan for deployment for the organization. Because this was a first for me with deploying such a big border crossing project I first choose to research the solution further and looked at the many whitepapers and case study's that are out on the internet.
In the time that I would be working on the project during the implementation I was relieved of the other duties I would normally do so I could focus completely on this project.

Rule of thumb:

- When you start rolling this project out be prepared and try to keep/get yourself out of normal operations.

Why that last rule of thumb here? Especially when you are faced with such a project with remote rollouts and so it is a relieve for your contacts to be able to call you the whole day through and not be "bothered" with you and your team being busy with something else.

Defining a structure:

After selecting Trend Micro for our AV defense in depth solution we asked ourselves the following question.
How could we define a structure for the whole protection scheme?
At first this may seem as a daunting task but if you get a grasp of the Trend Micro structure and the various roles the task will prove to be lighter.

Rule of thumb:

- When defining an infrastructure first look into the Trend Micro documentation on the different functions of the products.
  This will give you an answer where to place the different products.

As we chose Trend Micro and did some research, the group directors gave us a blank sheet in which way we would structure the whole av protection.

We opted to install a central site in the Netherlands. We chose Holland because I as the security administrator am based in Holland and the end responsibility for this project also lies in Holland.
So logical reasoning made the choice where to deploy the main site an easy task.

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

Rule of thumb for deploying a neatsuite solution:

- Install the main/management site where the responsible security administrators are based.

This may seem logical, but I've seen cases where the main site was deployed in a remote location with no psychical access.
Now how are you going to fix a problem when you can't access the system remotely? Normally you would only need remote access to the server but if that fails you will want to be able to access the server physically.
The issue with physical access is also an issue for the main serverprotect and officescan sites. Should you deploy them throughout your enterprise please be aware to host the system in a monitored environment.

For the main locations we defined a minimum number of workstations and servers as a guideline for deciding which sites would become a main 'country" site. If the location fell beneath that mark it would become a "sub" site.
You can limit the main sites if you have many small sites but be warned that you can't spread it too much cause that will bring together sites that might be to diverse.
Why I give you this advice is that it takes less network traffic to deploy a patternfile and/or scanengine to one officescan server then to 20 officescan clients so that if you get a certain number of workstations in one location you are better of with a separate officescan server in those locations. The same logic also applies for implementing serverprotect and its management server, the serverprotect information server.

Rule of thumb:

- When bandwidth is widely available it is advisable to limit the number of officescan servers and serverprotect information servers. When bandwidth availability (or lack of) is an issue a local implementation of an officescan server or serverprotect information server is recommended.
- What might be an option for your deployment is to define the main sites in the same matter as other enterprise wide deployments. For instance when you have main locations with sub sites supervised by those main locations. In this way you can keep the site definitions inline with the already existing defined sites.

What also needs to be taken into account the bandwidth the solution will use corresponding with the main serverprotect and officescan sites, every patternfile update and scanengine update will pas through these servers.
So before implementing please check the bandwidth requirements for such updates and if certain critical processes (e.g. Citrix) use the various intranet connections. At the moment we planned this project we checked all the intranet connections and noted the bandwidth available. We found no problems considering the plethora of bandwidth that was available.

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

Out of the research we did the following diagram was chosen as the structure for this project.

Glossary for the diagram:

The main management site provides the overview interface and the updates for the various programs used throughout the European enterprise.

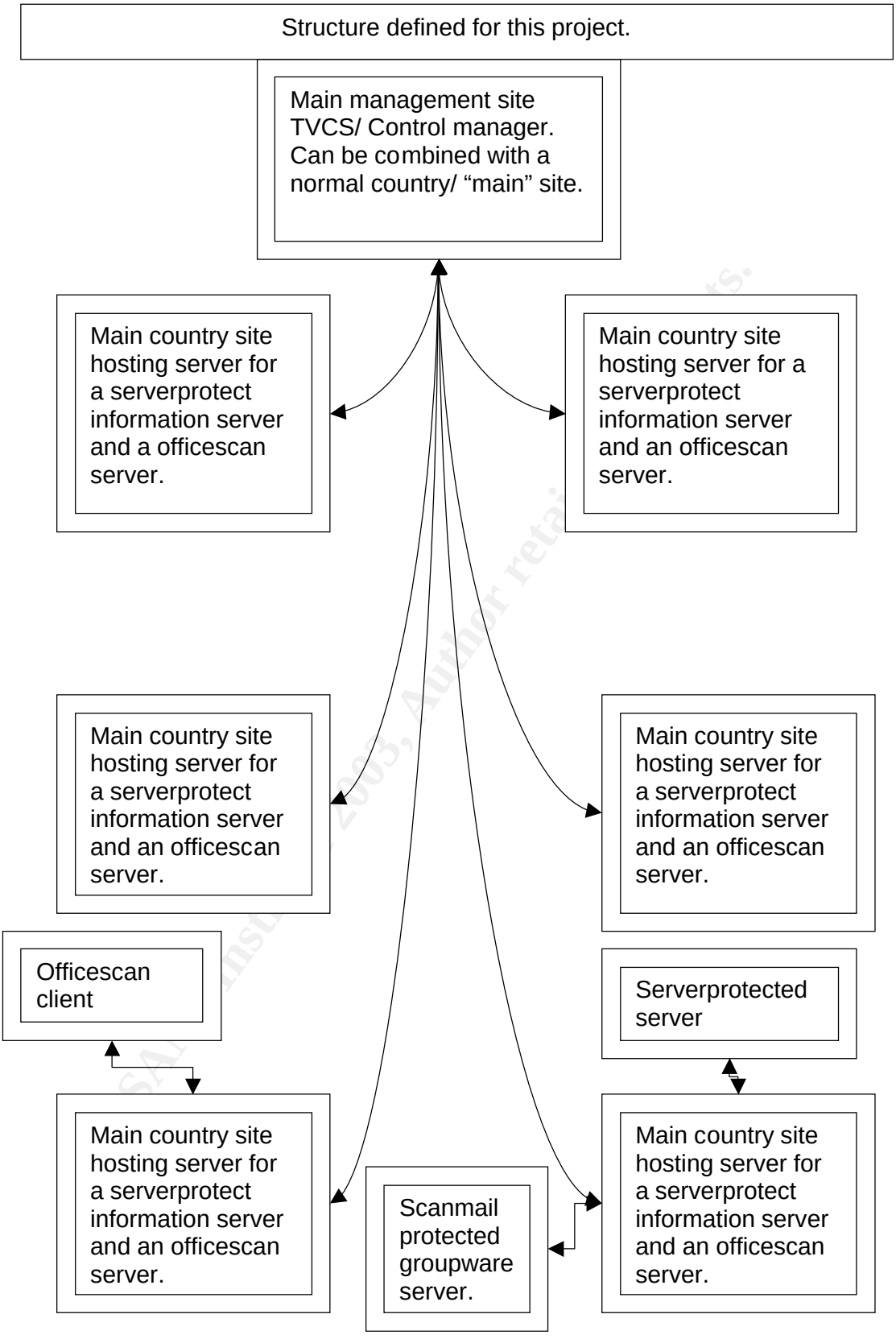
The “country” sites are the main locations in the enterprise where the biggest offices are located.

The “sub” sites are sites where the protected computers and servers are connected to a big “country” site
Why I put country in parentheses was that some locations serve more then one country as some offices are limited to a couple of computers they are managed and served by one of the bigger locations.

I also will put the diagram below into a simple text diagram in order for you to understand how things are organized.

- Management server
  - Main country site: Officescan server, serverprotect information server
    - Officescan client
    - Serverprotect protected server.
    - Scanmail groupware scanner
  - Main country site: Officescan server, serverprotect information server.
  - Main country site: Officescan server, serverprotect information server.
  - Gateway site: Interscan viruswall, location where SMTP and/or HTTP and/or FTP scanning are done

© SANS Institute 2003, Author retains full rights.



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

When planning the implementation of the antivirus project I made several arrangements in order to do a quick implementation.

During the rollout of the project I kept the responsible managers and IT contacts up to date on system ship status and so on. Besides keeping those people up to date on the status of the project I also made a completion notice form on a whiteboard with the infrastructure we chose. In this way we could keep our helpdesk up to date as well, so that anybody who called informing about the project status they were sure to get a quick and very important an accurate reply.

Rule of thumb:

- When deploying such a project make sure to keep your helpdesk/ service desk up to date.

Why we implemented the above rule was for a couple of reasons.
One major reason was that most of the installation was done remotely.
This might leave users in the dark sometimes when you don't inform them that you have changed the av protection. For instance we decided during planning to insert an automatic virus safe message into the subject of every mail coming into or leaving on of our mail servers. This was a first as that wasn't possible with the previous product we used on the domino server.

Rule of thumb:

- When deploying the systems please be sure that all the required contacts who have to do a share in this project are up to date and know what to do.

The reason I mention this is, when I was deploying a scanmail installation abroad I was confronted with a lotus notes/domino administrator who didn't know what he had to do. I did of course inform him beforehand what his part in the rollout was. Also a problem was that the involved administrator didn't speak proper English. So I couldn't communicate with him which led to a delay in the rollout.

Problems we ran into during deployment:

When in the first months of running a problem arose with some small locations where the bandwidth ran out. What was discovered is that those locations worked with terminal server/citrix clients on a cluster located in France. This wasn't mentioned before by the responsible IT personnel there. This had to be solved after complete deployment. At that time we solved it with some QoS service settings on the routers in those locations.

Also the language issue proved to be a bit of a show stopper but that was quickly solved as I was assigned a different lotus domino administrator.

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

After:

In the months following the project we used the input from the trend micro management the various responsible it administrators and selected key users around the company.
Some issues were the bandwidth problems in the smaller locations and some notifications of the various virus notification mails generated by the trend micro systems. Another issue was the lack of documentation and training for the various it contacts.

Bandwidth problems

As we ran into some troubles when deploying the solution at the smaller locations with the bandwidth, we decided to deploy a separate officescan and serverprotect server in those locations.
Because of the small numbers of workstations in those locations the officescan server was installed on a server already available there. This cut costs but if you would like the most manageability you are better off installing it on a separate server and not on a “shared” server.

Training/procedures issue

What also proved to be of some trouble was that the staff that was to support the solution locally where sometimes not adequately trained to support the products there. This may seem an implementation research error which you can figure out before hand but nothing tells the real truth then a live exercise.
We figured that because of a lead in time for the project the designated local administrators would have sufficient time to learn the products before rolling it out completely without requiring training
Solving this issue was proved quite easy as supplying them with the most commonly used procedures in our enterprise and giving them priority when calling our helpdesk for other problems.

Evaluation results

Virus incidents

The number of virus incidents reduced by the defense in depth approach was staggering to say the least.
How we could prove this was by comparing logs from the various systems and comparing them with the log data from the older solutions.
What proved to be elemental were the following items:

- More variants of known and new viruses detected (more efficient scanning process)
- Number of virus incidents reduced from 10-15 a year to 2 incidents in 1,5 year. Defense in depth decreased the vulnerability
- Drop in detected viruses at the desktop and fileserver level which originated from the fact that the gateway and groupware scanning was a lot more efficient.

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

With the new solutions we were able to secure any system a lot more efficient then before. Installation procedures including testing were under wraps in an hour.
On the fly installing of the av software was now also achieved.
What this meant that we could install during daytime instead of having to wait to install it off-hours. This meant that a server or application could be brought online securely online during the day as no reboots or intensive installation procedures were required.

The patternfile latency and deployment issue was also solved now.
At the moment our Trend Micro management console checks the active update site once every 15 minutes for a new patternfile.
Should there be a new patternfile available the entire solution will take approximately one hour to propagate the patternfile throughout the enterprise.

What this meant in short was that loveletter and a lot of other wide spread viruses were just stopped at the gateway level and wasn't even able to reach the groupware level or let alone the fileserver or desktop level.

When we implemented the trend micro solutions we also implemented a new av policy in the whole European enterprise. Every employee had to sign an agreement. This made every employee responsible for maintaining a secure work environment.

But to be realistic new vulnerabilities were also introduced with the new solutions. For instance the management solution TVCS/ Control Manager is based on IIS and SQL server 2000. Both products have a reputation for being buggy so this is an issue for you to consider.

Rule of thumb:

- Don't implement Trend Micro Control Manager when you don't know how to secure your IIS.

With the central management product TVCS a web interface was introduced what it meant in short was that armed with the password for accessing the interface one could manage but also disable parts of the av protection. You now longer needed access to a configured management terminal or server for that case. You could of course restrict acces to the website to a couple of specific ip addresses but being able to manage the solution throughout the whole enterprise was the main selection factor. So the webinterface proved to be a double edged sword when it comes to its administration ease.

When it comes to 0-day viruses vulnerabilities still exist but one that you will not be able to eradicate as even with heuristic scanning you will still be caught first before you can eradicate it.

The various serverprotect and officescan servers are protected by passwords.
As you all know, once you write down a password the affected system will be insecure. This means you have got to know who will administrate the solution.
Ideally speaking you will want each individual to go through some sort of a screening process.

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

Note:

While some of the names of the different applications mentioned in this paper may or may not be current at the moment you're reviewing this document I intended to provide them as is to provide as clean an overview as possible. But for reference when they are updated products now in place I will name them in the glossary.
Also the before section is based on research I did in 1999-2000 on the various solutions available at that time. Quick research on my part has shown that the 2 other vendors we researched have extended there offering and are in my opinion more of a competitor then they were in 1999. This casestudy can be used for your research but I urge you to also test the various solutions yourself.
I hope you benefit from the experiences I've had with the Trend Micro solutions so it will help you avoid some of the pitfalls I've encountered.
Please enjoy the read.

Glossary:

Information server:

A server which is the hosting server for a serverprotect installation. Protected servers are defined under such a hosting server.
E.g.:

- Serverprotect information server
  - Protected NT server
  - Protected Netware server

Officescan Corporate Edition.

The AV-solution from Trend Micro for the corporate desktop.

Serverprotect for NT/2000/.NET/Netware.

The AV-solution from Trend Micro for the corporate file and application server.

Scanmail for Lotus Notes/ Exchange.

The AV-Solution for the corporate groupware server.

Interscan Viruswall.

Trend Micro solution for deploying a HTTP, SMTP and FTP scanning solution at the internet gateway.

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

Trend Micro Control Manager (TMCM).

Administration, reporting solution for the enterprise av solution. Successor to Trend Micro Virus Control System. Now features encrypted agent communication, outbreak prevention and extended reporting in addition to the features found in TVCS

Trend Micro Virus Control System (TVCS).

The predecessor to Trend Micro Control Manager. Package for centrally managing and administrating Trend Micro antivirus products.

QoS (Quality of Service):

A way to provide traffic management on a network device (e.g. a router)

Defense in Depth:

Defense in depth refers to securing an infrastructure in layers. With defense in depth you build multiple layers of security measures to build an almost impregnable infrastructure. When one layer of security measures fails you are able to fall back on another layer of security. In antivirus protection this refers to integrated multi level av protection software. Trend Micro's Neatsuite is a example of such a software suite.

Patternfile:

A file consisting of definitions of the current viruses known to a supplier. These definition files are updated once new viruses are released and identified.
Through pattern analysis detection of new viruses are made possible.
Patternfile updates are because of its character one of the most important elements of an effective av infrastructure. Without a updated patternfile a av infrastructure will quickly become ineffective at stopping viruses.

IIS:

Internet Information Server. The webserver application from Microsoft. Known for frequent (security) bugs. Non secure installation by default. Requires administrator intervention to secure its webservices.

References:

Trend Micro whitepaper: "Implementing Trend Micro Control Manager" August 2002
Url: http://www.trendmicro.com/en/products/management/tmcm/evaluate/white-papers.htm 05 April 2003

Trend micro whitepaper: "Implementing Trend Micro Interscan Viruswall in a Stonesoft cluster environment" 07 November 2000
Url: http://www.trendmicro.com/en/products/gateway/isvw/evaluate/white-papers.htm 05 April 2003

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

Trend Micro whitepaper: Implementing Trend Micro Serverprotect for NT/Netware. Februari 2003
Url: http://www.trendmicro.com/en/products/file-server/sp/evaluate/white-papers.htm 05 April 2003

Use the link found in the aforementioned pages.
To read the above papers you will need Adobe acrobat. This can be found at: http://www.adobe.com/products/acrobat/readstep2.html

Castelli, Jacqueline "Choosing your Anti-Virus software" 2 April 2002
Url: http://www.sans.org/rr/software/anti-virus.php 5 April 2003

Bitton,Pat from Trend micro "Today's virus protection selection criteria guide" 02 November 1999
Url: http://download.antivirus.com/ftp/white/vir_prot.doc 05 April 2003

From Trend Micro "Designing and Implementing a Virus Prevention Policy: Key Issues and Critical Needs" 24 February 1999
Url: http://download.antivirus.com/ftp/white/policywp.pdf 06 April 2003

Gordon, Sarah "Reviews and Evaluation of Antivirus Software: The Current State of Affairs" 19 April 2000
Url: http://secinf.net/uplarticle/10/final.pdf 13 April 2003

Fedeli, Allan "Organizing a Corporate Anti Virus Effort" 28 January 1991
Url: http://secinf.net/uplarticle/10/fedeli.txt 03 April 2003

Index:

- Abstract page 2
- Before page 2
- During page 4
- After page 12
- Glossary page 14
- References page 15
- Index page 16

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