Global Information Assurance Certification Paper

Centralized Anti-Virus Management
ePolicy Orchestrator

Practical Assignment Version 1.4b
SANS Security Essentials CISSP

Brian Massie
June 19, 2003

Table of Contents

Introduction

This paper will introduce concepts of Malware and briefly describe the three main types, along with the damage they can cause to a computer system. This damage can cause anything from a minor disruption for one or two users up to damaging the credibility of an entire organization's reputation.

Companies realize they need to protect themselves against Malware by installing anti virus software. I will discuss the progression over the years as to how the industry has defended itself against viruses. The anti-virus industry and bigger organizations soon discovered that just installing anti-virus software on desktops and their server was not enough. They needed to become more pro-active as the viruses became increasingly damaging. In order to become proactive an organization has to know what the anti-virus situation is in the organization. This cannot be determined without a centralized management solution. ePolicy Orchestrator from Network Associates is one solution, which helps an organization understand how it stands on defending themselves against the ever-increasing threats from malicious code.

Malware, What is it?

Malware is the term used to describe a code, script or software that executes or runs something that the users had not intended [1]. This unwanted code, script, or software comes in a variety of forms from pranks to very destructive software. Malware is commonly referred to as a computer virus. This is a misconception of the general public, the press, and even some network administrators [2].

Pranks do not do any damage to your computer systems but the can cause people to panic and things that they shouldn't do. The JDBGMGR Hoax is prime example by getting the user to delete the JDBGMGR.EXE file. This has fooled a lot of users [3].

The most recent LovGate virus has become a real concern. It is capable of emailing itself out, modifying files, it drops a Trojan to allow unauthorized remote access to the infected computer, and it tries to disable a number of different anti virus software programs [4].

1 Chris Quirke
2 Bernie Klinder
3 Northunbriaonline
4 W32.HLLW.Lovgate.l

Types of Malware

Types of Malware are classified into many different categories based on how it replicates the way it executes, and its payload. Viruses, worms and Trojans are the best-known forms of Malware. The term 'viruses' is used as a generic name for all Malware but this is a mistake as there are differences between the types. It is important for administrators to know the difference between them in order to be able defend against them [5].

Virus

A virus is a program designed to spread and infect other computers with little or no user intervention [6]. Viruses can be harmless or they may be designed to cause a lot of damage such as formatting the user's hard drive [5]. "Viruses falls into one of four categories: boot sector, program, macro, and multipartite viruses" [7].

Worms

Worms are similar to viruses except in the way they replicate. A worm is spread without modifying or attaching itself to a host program. Worms create copies of them and then send the copies via email or Internet Relay Chat (IRC) [8].

Trojans

Trojans are programs designed to trick users. They masquerade as harmless programs but instead these Malware programs are far from harmless. Trojans use social engineering as a means to have the user launch the program. Early Trojans did not replicate themselves but the new variants are becoming more sophisticated so that they can launch worm/virus hybrids [5].

Defense against Malware

For years it has been considered important for companies to install anti-virus software on user's desktops to defend against viruses, worms, and Trojans. Later

5 Bernie Klinder
6 McAfee
7 Types of Computer Viruses
8 Computer Worms and Viruses: Is Your Network Next

on, anti-virus software was developed for the e-mail gateways and file servers. This added another layer of defense against Malware. Having anti-virus software on the e-mail means those viruses can be detected, cleaned or deleted before they reach the user.

This multi-tiered layer of virus protection soon became less effective as the virus writers came up with more sophisticated methods. Viruses like the SQL Slammer worm are starting to target vulnerabilities of systems. "They also are beginning to be file-less and only reside in memory" [11]. Therefore, gaps formed in the layer of defense, which needed to be identified and addressed.

Gaps in Non-Centralized Anti-virus Management

Defending against Malware means more than just installing anti-virus on email gateways, servers, and desktops. In small to medium sized companies this may be enough. The number of computers is small enough that managing the anti-virus software is possible. However, in larger companies, management of the anti-virus software soon becomes a challenge. Another challenge is the deployment of the software and the upgrades.

Organizations may have one or more methods, which they can use to deploy their anti-virus software and scan engines. These solutions, depending on the methods, involve a lot of planning, collaboration, and cooperation among different groups within an organization.

Without a centralized anti-virus management system management staff cannot fully know or understand the anti-virus posture within their organization. For the most part, all that mattered to management was having the anti-virus software installed on the servers and desktops. Now it is critical for management to understand the anti-virus posture. In order for management to have a better understanding they need to have regular reports. These reports would have to include the following information:
1. Does a machine have the proper software installed? 2. Is the software being updated regularly? 3. Which machines are being infected? 4. What virus is infecting the machines? The management staff is not able to obtain this kind of information without some kind of centralized management tool.

Without having a centralized management tool gathering this type of information is time consuming and expensive. The process involves a lot of manual labor ranging from compiling data for GroupShield logs of a range of server to either physically walking around to each workstation or compiling a script to obtain

11 Robert Vamosi

information about the user's current anti virus status.

Centralized Management Tools

Having a centralized anti-virus management tool provides an organization with the means to easily deploy anti-virus software, to enable upgrading of scan engines more efficiently, to provide administrators with a way to manage their policies across the entire enterprise, and to provide management with detailed reports of the anti-virus posture. It also allows for virus outbreak management. In the event of a virus outbreak an enterprise-wide deployment of all the most current anti virus software and DAT files can be pushed to all computers. Reports can be generated to show the extent of the outbreak and the point of entry of the virus.

Introduction to ePolicy Orchestrator

EPolicy Orchestrator (ePO) is a centralized management tool which provides an organization a means to manage and enforce anti virus policies, to deploy anti virus software, and to be able to have reports showing the anti virus posture solution from a centralized location [12]. Centralized management allows administrators to manage their anti-virus policies for groups of computers or for a single user, and it provides many types of reports to allow management to see the overall anti-virus posture of their organization. The management of the organization's anti-virus state is done through a single console or multiples consoles, depending on the configuration, from anywhere in the enterprise.

"ePO is a product of Network Associates Incorporates (NAI). ePO manages NAI anti-virus products VirusScan, NetShield for Netware and Windows, and GroupShield 5.0 for Exchange 5.5/2000 and Lotus Domino 5.0a and WebShield appliances. It also supports Symantec Norton AntiVirus 5.0x/Corporate Edition 6.0x for Windows" [10].

Components of ePO

ePO consists of 4 main components: Server, console, agent and database.

12 Network Associates

The Server

The server makes centralized anti-virus management possible. "It gathers the properties from the agents and sends it to the database and it also relays the policy from the database to the agent" [13]. The server allows the administrator to separate the users into groups according to the organization's anti virus policy management. A single server can be used to manage up to 250,000 machines allowing it to be very scaleable [14].

The Console

The console allows the administrator to manage ePO from any Windows NT4.0 workstation or Win2K platform. "It uses the Microsoft Management Console" [13]. The database stores the information about the machine, which the agents are installed on, and it gives the graphic Directory Tree Structure which agents are installed on the machine through the console.

The Agent

Each desktop and server has to have an agent installed on it. This agent provides the centralized management system with the client's anti-virus configuration. The agent gathers information about the machine, the anti-virus software, and configuration (policy) and sends it to the server on a regular basis. "If the policy on the machine doesn't match the policy in the database the agent can enforce the proper policy" [13].

The Database

ePolicy Orchestrator stores the data collected from each agent and then displays the information about each client in a directory tree structure through the console [12].

13 Lee Fisher
14 McAfee

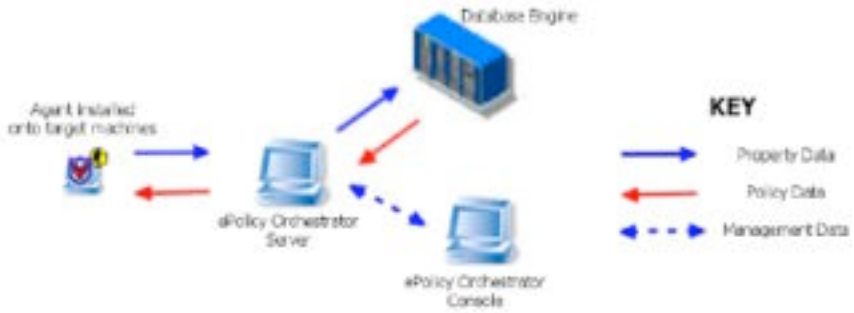

Figure 1: Illustrates Date Collected from Agent [13]

Microsoft Data Engine MSDE or Microsoft SQL Server 7.0 with service pack 7 or Microsoft SQL Server 2000 can be used for the database. MSDE can be used for 2,000 agents or less and for more than 2,000 agents it is recommended using MS SQL server.

Installation Requirements

These are the minimum requirements needed to get ePolicy Orchestrator up and running. To insure that you have a robust infrastructure that can handle any additional increase in the company's growth exceed the minimum requirements.

Server and Console System Requirements

Operating System	Windows NT 4.0, SP 5	Windows 2000 Advanced Server, SP1; or Windows 2000 Server, SP 1
Processor (250 nodes or less)	233MHz	
Processor (250 nodes or more)	500MHz	Dedicated server
Free Disk Space	1GB	
Partition	NTFS	
RAM	128MB	

Table 1: Server and Console System Requirements [13]

Agent System Requirements

Operating System	
Windows 95/98	Windows 2000 Server, SP 1
Windows NT Server 4.0, SP 4	Windows 2000 Professional, SP 1

Windows NT Workstation, SP 4	Windows Me
Windows NT 4.0, SP 5	Windows XP Professional
Windows 2000 Advanced Server, SP 1	

Table 2: Agent System Requirements [13]

Managing Anti-Virus Policy Through ePO

To manage anti-virus protection in an enterprise using ePolicy Orchestrator, an agent must be installed on the client's machine. Once the agent has been installed, policies can be set. Policies are configurations for the agent itself and for the product (For example VirusScan or NetShield). The administrator has the option to have the policy enforced or not to have it enforced. If the policy is not to be enforced then the agent is only used for reporting.

"Policies can be set on the whole directory tree structure (Global Policy) or by group (site) or even individual computers (nodes)" [13]. Creating a global policy will insure that all users will have the proper policy. The global policy is created at the root directory. Any site or node that is added to the root directory would automatically inherit that policy.

Figure 2: Modifying Policies [13]

Individual sites, groups, and even computers can have their own policies separate from that set at the root level. Setting different policies for servers, desktops, laptops, and even groups of computer in different areas is necessary because servers need different configurations than desktops and laptops may need their own configuration if they use remote dial-in access. If the company is wide spread and uses local FTP servers for updating DAT files, each site can be configured to point to its own local FTP server.

EPolicy Orchestrator uses the agent to manage the policy. The agent is configured before it is deployed. There are several options for the agents and for events.

The agent has four configuration settings. "They are: 1. Agent icon appears in the system tray. 2. If a reboot is required the user can be prompted. 3. The interval in minutes in which the cached policy is enforced on the local machine. 4. The interval in minutes at which the agent communicates with ePolicy Orchestrator to obtain update in the policy. The last option allows the administrator to be able to contact the agent for the ePolicy Orchestrator" [13].

Figure 3: Configure settings and policies for clients [13]

Agent-to-Server Communication Interval

"The agent-to-server communication interval (ASCI) determines how often the agent sends computer properties to and receives policies and tasks from ePolicy Orchestrator server" [13]. If the agent detects any changes to the policy it will only send the changes, not the whole policy. This reduces the network bandwidth requirements needed.

The Agent - How it Works

"When the agent is installed onto a clients computer, it collects the machine properties (the machine's Net BIOS name and the MAC address) and sends them to the ePolicy Orchestrator server" [13]. Since this is the first time the agent communicates with the ePolicy Orchestrator server an agent ID is generated. This ID is a 64-bit key and is used for all other Agent to Server communication to identify that particular agent. This is to make sure that a machine only has one entry in the directory.

The agent then starts collecting information on the machine's configuration. This information includes the machine's IP address and operating system version among other information, which it sends to the server. It then receives the agent's configuration policy from the ePolicy Orchestrator server as well as configurations for other products such as VirusScan and NetShield, which may be installed on the machine. If the local configuration does not match the configuration from the server the agent enforces the policy.

If the machine doesn't have a McAfee product installed, the agent can download the

product from ePolicy Orchestrator.

Deploying the Agent

Deploying the agent presents the greatest challenge to an organization. The organization structure and the kinds of operating systems used have a bearing on how best to deploy the agent.

Organizations with domain have an easier time deploying agents than ones that do not. If NT domains are not in an organization then the agent cannot be deployed via the ePolicy Orchestrator. Other options, such as a manual deployment, or enterprise software management solution, like Tivoli or Novell Application Launcher has to be used for the deployment. This would mean a lot more thought and planning is necessary to make the deployment possible. A combination of methods will insure that workstations receive an agent.

Tasks Management

Tasks are used to do something immediately or sometime in the future. It can be anything from updating DAT files and upgrading the scan engine to running an on-demand scan. When a task is scheduled through the ePolicy Orchestrator server it runs without the user's help. It is hidden from the user.

Creating a Task

To create a task you need to select an object in the directory tree. Right-click the object and select S*chedule Task*. Name the task something that identifies the task. If you were creating a task to AutoUpdate your DAT file, a good name would be your company's name and the name of the task XYZ AutoUpdate, for example.

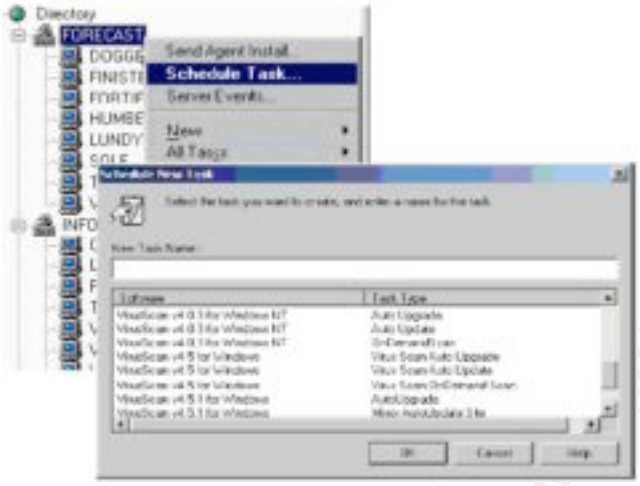

Figure 4: Configuring a new Task [13]

Each McAfee product has a specific configuration. Choose from the drop down menu the task that is for the product that you are using. This is necessary to have the correct configuration for the product.

Scheduling Tasks

There are several options that ePolicy Orchestrator gives you to run a schedule task. If your company has a certain policy for the desktops and another one for the servers and another one for laptop, each of these can be scheduled to be updated automatically. It ranges from running the task immediately, to running it monthly, or to running it just once.

Configuring an AutoUpdate Tasks

AutoUpdate is a task that is run to update your DAT file. An organization may use different option to update their DATs. They can be retrieved from UNC path, FTP site or a local path depending on the organization preference.

As with scheduling a task, configuring the AutoUpdate task requires that you name the task with something relevant.

Reporting

In order for management to have a better understanding of the anti-virus posture in their company they need to have a way to get reports. ePolicy Orchestrator

provides 35 different types of reports. They are separated into two groups. The first is coverage and the second is infection.

The main things coverage reports show are what agents are communicating with the ePolicy Orchestrator server, how many machines have up-to-date DATs and engines, and what percentage of the machines are up-to-date. It provides information as to how and what kind of coverage the company has.

The main reports are Agent-to-Server Communication Information, DAT/Definition Deployment, DAT Engine Coverage, and Engine Deployment Summary, and Product Protection Summary [12].

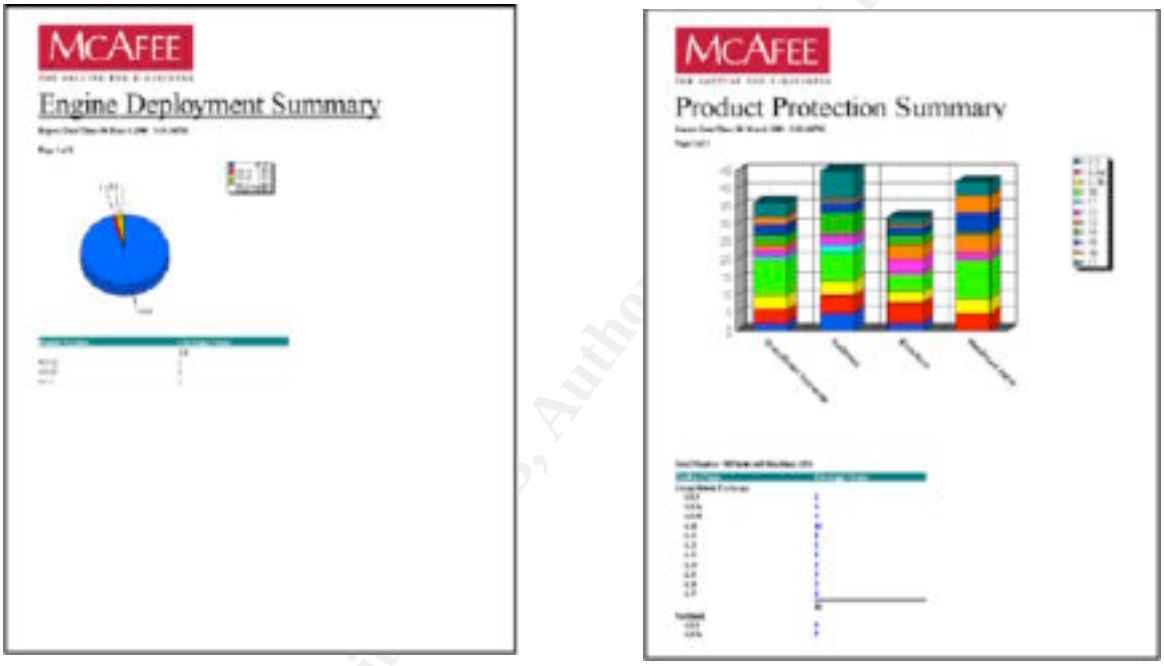

Figure 5: Samples of ePO Reports [12]

Case Study

Installing the Agent

Problem

Upon the deployment of ePO it was discovered that there was recently a new DNS suffix being used in the enterprise. Most of the existing users have not added the new suffix to their configuration. As a result the ePolicy Orchestrator agent could not resolve the new suffix preventing the agent from communicating with the ePO server.

Background

The deployment of the agent as mentioned above can be done in several ways. The easiest and fastest way to deploy agents is to have an environment, which has domains. If your company does not have domains then deploying agents is more challenging.

Once the deployment option has been decided upon and the deployment is set to start, most companies proceed with the deployment without a thought and things go smoothly. However, sometimes problems can occur that can take time to figure out. One such issue has to do with not using the correct DNS suffix. This issue isn't a normal issue that many companies would be faced with, but it can happen. Of course, before any installation of a new application into a production environment, various tests are done in a lab environment. Here, any bugs in the application are discovered along with any problems with the installation, agent deployment, or any other issues with using the application. Lab environments are good for testing but they are not always the best environments for finding all the issues involved in using ePolicy Orchestrator.

Solution

The testing of ePolicy Orchestrator in the lab environment went smoothly and didn't uncover any major issues, but as soon as it was installed in the production environment problems arose. In one particular case, the deployment of the agent to the desktop went ok. When the agent is first installed it communicates back to the ePolicy Orchestrator server telling the server that it is out there and passing on the machines properties. It is not until the configured length of time that the agent again communicates to the server. This second agent-to-server communication was not happening in the production environment. After many discussions and tests in the lab a conclusion was reached that there was a DNS issue.

If a company changed to a new DNS suffix and hadn't been able to refresh all of the desktop images, this could affect the agent-to-server communication. The new DNS suffix has to be added to the local computer before the ePO agent is installed.

Summary

Encountering such a problem with the ePO agent not being able to communicate with the ePO server after the initial communication is rare. This issue aroused due to the fact that the DNS suffix in the organization was being changed at the same time the ePO deployment began.

NATed IP Address

Problem

Creating customized agent installation file (POAGINST.EXE) with the ePolicy Orchestrator behind a firewall caused the agent to not be able to communicate with the server once the first communication has occurred.

Background

When the agent customization file (POAGINST.EXE)is created the IP address of the ePolicy Orchestrator server is used in the customized file to allow the agent to locate the server. When the ePolicy Orchestrator server is placed behind a firewall, a NATed IP address 10.43.125.44 is used instead of the address of the ePO server 172.1832.15. Without the NATed IP address in the agent customization file (POAGINST.EXE), the agent cannot locate the server therefore the agent is not able to communicate with the ePolicy Orchestrator server.

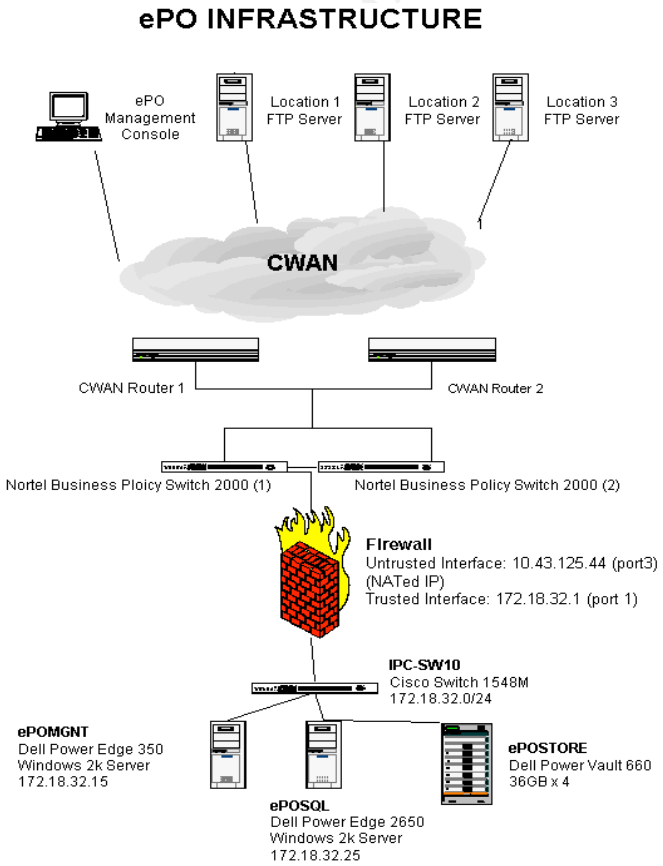

Figure 6: ePO infrastructure when ePO is behind a firewall [16]

Having the ePolicy Orchestrator server and SQL server behind a firewall an additional level of security added.

Solution

To solve this problem the agent has to be created with the NATed IP address of 10.43.125.44. Therefore, before the agent customization file (POAGINST.EXE) is created the IP address of the ePO server is changed to the NATed address. Going in the network properties on the ePO server and changing's IP address to the NATed address accomplish this.

To create the agent customization file (POAGINST.EXE) login to the ePolicy Orchestrator console and right-click ePolicy Orchestrator in the console. Select All Tasks and the Customized Agent Package. The Agent Configuration wizard opens allowing the agent installation file to be created. The agent customization file (POAGINST.EXE) is then saved to a floppy disk for manual distribution.

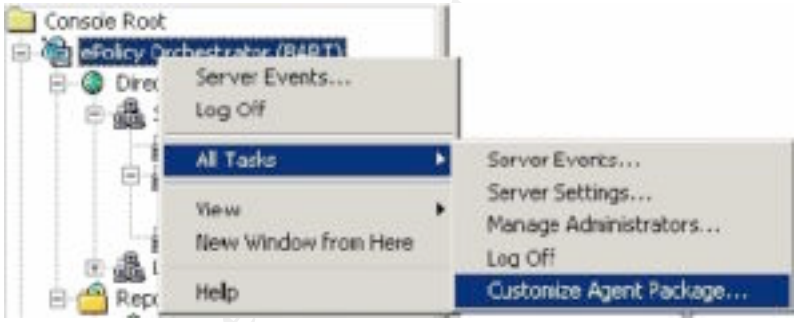

Figure 7: Creating a customized agent package [13]

Summary

When the ePolicy Orchestrator is put behind a firewall the agent uses the IP address of the internal assigned IP address. In order for the agent to be able to communication with the ePolicy Orchestrator server it will need the NATed IP address of the firewall.

Blue Screen

Problem

After the ePolicy Orchestrator agent is installed on a laptop or desktop some users experience blue screens or continuous rebooting of their machines.

Solution

Network Associates, Inc, (NAI) recommend to exclude the ePO agent directory from being scanned.

Summary

To avoid future problems for blue screens or continuous rebooting of machines which will have ePO agents installed it is recommended that for users to configure their VirusScan to exclude scanning the ePO agent directory.

Blue Screen

The procedure to exclude the scanning of the ePO directory to eliminate blue screen during startup is as follows:

1. Double click the V-Shield in the System Tray.
2. With the "System" tab highlighted click "Properties".
3. In the "System Scan Properties" window, click the "Exclusion" tab.
4. Click the "Add" button and then browse the directory and select the "ePO Agent" directory.
5. Click "OK" twice and close the window.

Continuous Looping

The procedure to exclude the scanning of the ePO directory to eliminate continuous looping during startup is as follows:

1. Double click the V-Shield in the System Tray.
2. With the "System" tab highlighted click "Properties".
3. In the "System Scan Properties" window, click the "Detection" tab.
4. Under the heading "Scan floppies on", uncheck "Access".

Console Connectivity

Problem

The ePolicy Orchestrator console cannot connect to the ePolicy Orchestrator when the console is installed on a computer.

Solution

ePolicy Orchestrator allows the management of anti-virus software from anywhere in the enterprise. The management of the anti-virus is done through the console. It allows an administrator to manage anti-virus remotely from any computer.

Before the console is installed, the local computer may require some configuration. The first thing is to configure your HOSTS file to include the entries for the ePO server and the SQL server (if you are using a SQL server). It might be necessary to add the SQL server name to the ODBC Data Source in the System DNS. Finally, the proxy server needs to be configured. Click "*Use automatic Configurations Script"* in the Internet Options, Connections, and LAN Settings.

Port 1433 needs to be opened on the firewall in order for the ePO to connect to the server. For security reasons, this port should only be opened to the IP address of the machine where the console is installed.

Summary

Ensure the above configurations are done before installing the console.

Summary

For an organization to became proactive instead of being reactive when it comes to anti virus protection, it has to have the tools to monitor the anti virus protection within its infrastructure. Having anti virus software on the desktops and servers and an anti virus policy does not guarantee an organization that it is protected.

For different reasons the anti virus policy is not or cannot be followed or enforced. Whatever the reasons are this creates an opening for Malware to enter the organization's infrastructure. An infection, no matter how minor, has the potential to cause a loss for an organization.

Centralized management applications, like ePolicy Orchestrator, are now available to allow for the management of anti virus protection centrally. This is a great benefit. Now, rather than hoping that every desktop or server has up-to-date anti virus software and DAT file, ePolicy Orchestrator can be used to determine if all the machines have their anti virus software up-to-date. Any deficiencies can then be corrected and the company is safe from loss of money and reputation.

References

1. Quirke, Chris. "About Malware." December 2000.
   URL: http://users.iafrica.com/c/cq/cquirke/malware.htm (May 24, 2003).

2. Klinder, Bernie. "Computer Virus and Malware Primer for Network Administrators." 1999 –2003.
   URL: http://www.labmice.net/AntiVirus/articles/avprimer.htm (May 24,2003).

3. Northunbriaonline. “Software Virus Hoaxes: Not just Harmless Pranks.” May 31, 2003. URL: http://online.northumbria.ac.uk/central_departments/it_services/its_hoax.htm

4. Symantec. “Symantec Security Response – W32.HLLW.Lovgate.I@mm.” May 31 2003. URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.lovgate.i@mm.html

5. McAfee, URL: http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/virus-glossary.asp#v (May 24,2003).

6. “Types of Computer Viruses” URL: http://www.taalaibek.no-frills.net/types_of_computer_viruses.htm (June 12, 2003).

7. “Computer Worms and Viruses: Is Your Network Next.” December 2002. URL: http://www.ibew.org/stories/02journal/0212/p12.htm (June 12, 2003).

8. Vamosi, Robert. “SQL Slammer Slows Internet traffic.” 27 January, 2003. URL: http://www.cnet.com/software/0-7760531-8-20820927-1.html?tag=txt (3 May 2003).

9. “ePolicy Orchestrator, A Whole New Level of Anti-Virus Management from McAfee.” URL: http://www.mcafeeb2b.com/common/media/mcafeeb2b/us/products/pdf/wp_us_epo_whole_new_level.pdf (31 May 2003).

10. “McAfee ePolicy Orchestrator FAQ’s.” 2002. URL: http://www-tus.csx.cam.ac.uk/virus/ePOfaqs.html (May 24, 2003).

11. Fisher, Lee. “ePolicy Orchestrator Walk Through, Version 1.91.” December 2001. (April 3, 2003).

12. Fisher, Lee. “ePolicy Orchestrator Walk Through, Version 1.91”, December 2001. (April 3, 2003) Link broken June 11, 2003

13. “ePolicy Orchestrator, A Whole New Level of Anti-Virus Management from McAfee”. URL: http://www.mcafeeb2b.com/common/media/mcafeeb2b/us/products/pdf/wp_us_epo_whole_new_level.pdf (March 26, 2003) Have to fill out a form in order to access the paper. Link broken June 14, 2003

14. Fisher, Lee. “ePolicy Orchestrator Walk Through, Version 1.91”, December 2001. (April 3, 2003) Link broken June 11, 2003

15. Fisher, Lee. “ePolicy Orchestrator Walk Through, Version 1.91”, December 2001. (April 3, 2003)

16. Massie, Brian. The Author June 3, 2003