Global Information Assurance Certification Paper

Virus Defense in the Enterprise

Sans GIAC Security Essentials Certification
Version 1.4b
Option 1

By Daniel Van Meter
Completed December 25th, 2003

Table of Contents

Abstract

Today's enterprises are being threatened at an alarming rate with malicious code called "viruses" that can spread fast and carry costly payloads. Without an effective virus defense, companies may find themselves in a position of lost revenue, critical information, and confidence from customers and\or partners. This paper will provide a strategy for enterprises to manage their virus defense.

Enterprise Strategies for the Virus Defense

All enterprises should have a contingency plan documented and consistently followed in order to prevent viruses from infecting its systems. The strategy should consist of several layers of protection to provide an effective defense. The layers of protection can be broken down into the following three areas: network level, system level and user level.

Network Level

The first area an enterprise should concentrate its virus defense is at the network level. Preventing viruses from entering a network should be the main focus of any virus defense strategy. Some areas to look at are policies, network design, firewall and routers, and packet analysis.

Policy

Enterprises should enforce a policy that prevents unauthorized networking equipment from being installed. A network defense can be circumvented by poorly configured networking equipment such as wireless access points, routers, switches and hubs. Administrators and users should have authorized networking professionals install all networking devices with a secure configuration.

Network Design

Proper design of an enterprise's network can help in the prevention or containment of viruses. Before an enterprise can effectively protect its systems from a malicious code, an administrator needs to be aware of where the network parameter begins and ends. All doors in and out of a network should be documented and have ample protection provided. If companies use wireless networking devices, special consideration should be given to how far the signal reaches and what devices can connect to the access points. Wireless technology can be an asset to a company, but if not properly implemented can leave a network parameter open to hackers and viruses. It would also be wise

for administrators to be able to segment off critical systems from other areas of the network and provide additional protection and monitoring of such systems.

Firewalls and Routers

Doors that allow access to a network need to be protected by proper firewall and router configurations to block unwanted traffic. Routers and firewalls should only allow traffic through ports that are needed for the enterprise to properly function. This can reduce the number of pathways viruses can take and can reduce logging with packet analyzing software.

Users connecting to the network from VPN, wireless, and dialup all pose a risk to a network's security since they open the network's parameter to systems that are lacking the enterprise's virus defense strategies. An administrator can help provide security to a network by segmenting these systems on the network and allow stricter firewall and router rules.

Packet Analysis

Many packet analyzing products, also called Intrusion Detection System (IDS), are available to help administrators in the detection of many forms of intrusions to a network. Malicious code can be greatly reduced by placing the device in front of, but not limited to, all doors that may allow outside information into a network. The IDS should be behind a firewall or router to allow the product to not become overwhelmed with all of the data entering the network but only the data that is being filtered from a higher level device. Additional hardware devices should be placed in areas of the network to monitor systems based on importance such as a server segment. This can help reduce critical servers from being exposed to malicious code or attackers by notifying the administrator when an event occurs. By performing packet analysis on an enterprise's network, an administrator may be able to prevent the spread of viruses by properly reacting to early warnings of suspicious events. This paper will cover a software and hardware method of intrusion detection that is available to businesses.

Snort [1] is a popular open source network intrusion detection software that is free, thus its wide popularity. It is capable of real-time network traffic monitoring and can alert administrators of suspicious traffic on an IP network. Snort uses rules to describe traffic and then logs any packets that match the rule set.

ISS [2] provides a hardware solution called the Proventia G and M series that in active mode acts as an inline device, inspecting all incoming traffic. The Proventia G & M series is designed to log malicious signatures, block network attacks, intrusions, viruses, spam, and other unwanted traffic.

Systems Level

Network design cannot address all the possibilities of virus outbreaks in an enterprise. For this reason it is important to provide protection at the system level in a network. There are several methods of providing protection at the system level and an administrator should use a blend of such techniques. All operating systems should first be securely configured with an industry best practices reference. The next focus should be to implement a system level policy, deploy antivirus software, provide a patch management solution, install a system level firewall and regularly scan systems to provide countermeasures for viruses.

Policy

A policy should be defined to prevent unauthorized systems and devices from being connected to an enterprise's network. This is desirable since such systems may not have the proper antivirus software, security patches and may contain software such as file sharing programs which are known to circumvent firewall and routers.

Antivirus Software

It is vital that all operating systems in an enterprise have some form of antivirus protection. Although the Windows operating system has incurred the most viruses to date and may be the largest population of an OS in an enterprise, other operating systems such as MAC, LINUX, UNIX, and SOLARIS have all had viruses written specifically for them. Companies should never protect systems based on what the current virus threat is, but rather based on what could potentially be a threat in the future. All operating systems contain code that poses the threat of manipulation. It may be devastating for a company to be exposed to a new threat to an operating system and have no licensed software to deploy and the education to support such a product. With the growing popularity in PDA technology, enterprises should take additional precautions by providing such devices with antivirus protection since a user may transfer an infected file to a company's systems. There have been a few viruses written spefically for PDA devices. "Three main viruses have been found: Vapor, Phage, and Liberty Crack" [3] .Many antivirus software companies have introduced virus protection specifically for PDA devices.

All enterprises should scan email messages entering and exiting through its servers. Many viruses are written to spread through email and then use social engineering tactics to trick individuals into opening and executing the virus. Files that contain extensions that can execute an unknown program should be blocked from all inbound and outbound email servers.

There are many antivirus products on the market today. An enterprise should evaluate several products for their effectiveness and install the antivirus software on all desktops and servers. Network Associates Incorporated (NAI) offers an antivirus software called McAfee [4] to protect many different OS versions. Also available in conjunction to McAfee is ePolicy Orchestrator, a centralized policy management program that works with most of NAI's security products. McAfee and ePolicy Orchestrator combined can provide optimal protection by offering administrators the following capabilities:

- the ability to create custom installations with settings that are optimal for that particular business and quickly modify the settings globally or individually if needed
- the ability to scan all messages that are received or sent from an enterprise's email server
- the ability to scan particular files or all files written to a system through on access scanning
- the ability to deploy updated virus definition immediately upon release from the antivirus company
- the ability to report when and what systems have been infected. It can also allow an administrator to know what version of McAfee antivirus is installed on systems and what definitions machines are running
- the ability to upgrade systems with patches and newer antivirus products.

Whatever product a company chooses, the capabilities listed should be considered in order to provide an administrator with an easy and effective way to protect systems.

Antivirus software is important and is the most common approach to protect systems; however, it is merely a reactive way to defend an enterprise's data from viruses and is why it should not be the only method of protection. To explain, first a virus is released and spreads throughout a number of systems before being detected. At this point an antivirus software company creates and releases a definition for its product to be able to detect the signature of the virus and effectively clean the system. Not all malicious code is detected by the antivirus software leaving some forms of viruses still able to infect systems. Today's viruses have the capability of spreading extremely fast and it can be a constant race to get virus definitions to all machines on a network. Systems may become saturated by viruses before a definition can be written and deployed in an enterprise.

Patch Management

Many viruses exploit flaws in an operating system in order to carry out their payload. Once a flaw is reported, a virus outbreak is expected that utilizes the flaw to quickly spread. Therefore, it is vital for an enterprise to monitor and maintain systems with the most current patches. Even without antivirus software, the Blaster and Nachi viruses would not have been able to infect such a large number of Windows NT/2000/XP operating systems if the Microsoft RPC patch had been installed.

Many products are currently on the market to aid an administrator in deploying patches to systems quickly upon release. Such products include Shavlik's HFNETCHK PRO, St. Bernard's Update Expert and Ecora's Patch Manager. Microsoft itself has recognized that its current method of utilizing the Microsoft Windows Update website has remained ineffective since most users are unaware of the importance of applying such patches or remain unsure of how to do so.

Microsoft had created the highly unadvertised free Software Update Services 1.1 (SUS) [5] which allows companies to setup Windows systems to automatically download and install critical patches to Windows 2000, XP, 2003 systems pending an administrator's approval. The SUS product can also benefit enterprises by having all its systems install patches from a local server rather than each one utilizing the internet bandwidth. Since the Blaster virus, Microsoft has diligently been working on its new version of the free Software Update Service 2.0 product which will allow administrators to patch not only the Windows critical patches on a system, but most of Microsoft's business software including Office, SQL, IIS, and Exchange. Microsoft had temporarily put a hold on the release on the beta version of SUS 2.0 in order to get feed back from its customers. A final product release is expected to be available in the first quarter of 2004 and Microsoft has stated that it plans to highly promote its product in order to insure that administrators have a way to protect Windows operating systems[6].

Enterprises should not just focus on patch management for the Windows operating system. All operating systems companies release patches that fix security flaws as well as operating system functionality. An Administrator should identify all of the different operating systems on the enterprise's network and setup a contingency plan for applying patches once released.

System Firewalls

Many viruses have the capability to spread through system ports. By controlling what ports are open on a computer with a system level firewall, an administrator may be able to prevent the infection of some viruses. There are many system level firewalls on the market today. Some of the more popular firewalls are BlackIce Defender, ZoneAlarms, and McAfee Firewall. Before deploying a

system level firewall an administrator should evaluate the product extensively to insure that legitimate software is not prevented from functioning normally on its computers. Many firewalls now include the ability to report and deny any application attempting to access information outside of the system through a particular application. Some important questions to ask when researching a firewall program for an enterprise are:

1. Will this interfere with the company's business needs? A system firewall deployed in a large environment can cause major problems for an administrator if it is not properly installed and configured. Individuals may find themselves locked out of systems and/or have legitimate business applications blocked from communicating to other systems. It is important that an administrator be highly educated in how to configure, deploy and maintain a firewall program.

2. Does an administrator have the ability to control the system firewall settings from a central location? It can be time consuming to adjust firewall settings on hundreds or even thousands of machines manually if a new threat arises. An administrator should be able to globally change firewall settings on many systems quickly in order to protect them from a new threat.

3. Will user interaction be required? Many users will not know what actions to take and may be alarmed if a firewall requests them to determine if certain traffic is to be permitted. Inadvertently, users may block legitimate activity and cause many problems for themselves or for the administrator.

4. Is centralized reporting available? A centralized reporting method in which an administrator is alerted of suspicious activity on systems can help provide quick responses to threats and allow an administrator to be proactive when the first few signs of intrusions are detected.

With these questions answered, a system firewall can be a major security enhancement for an enterprise's virus defense. Microsoft has included a firewall with its Windows XP and 2003 Server release. The firewall can provide adequate protection from inbound traffic; however, it provides minimal capabilities in blocking outbound traffic and provides little logging and remote management. Microsoft plans to increase security for the Windows XP operating systems in a service pack 2 release by defaultly turning on a newly enhanced firewall and increasing its manageability[7]. This may provide a comfortable level of protection for an administrator to protect systems from some types of viruses.

System Scanning

Administrators should consider running a system scanning product, such as Nessus[8], to find machines on a network that may be vulnerable to viruses or other intrusions. Nessus is a software provided free to an indivual that allows them to scan their networks for many different systems that are vulnerable to exploits. Nessus will analyze each open port and determine what services are running. It can determine vulnerabilities by actually executing the exploit on a system rather than assuming the system is vulnerable through banners or open ports. This can reduce the number of false positives reported. Once Nessus detects a vulnerable machine, it will log the system and provide an administrator with information on how to correct the security risk. Nessus can also be useful to administrators in finding machines that do not have critical patches installed or have services that are running that may be exploited.

User Level

Even with a good network design and system protection, viruses potentially can still find their ways into a network and onto systems. The last line of defense lies with the administrator and user and therefore enterprises should provide a written policy and education to all members within the company.

Policy

An enterprise should have a policy available that clearly defines how a user should report viruses or any other suspicious activity on a system. When confronted with a virus, it is recommended to have users contact an administrator to verify, document and clean the system. Failure to follow this procedure can result in damage to systems through hoaxes and ineffective cleaning methods. Administrators should report any virus that poses a security risk to a Network Security Department or higher authority if the virus allows an unauthorized individual to have remote access to a system or if compromise and/or damage to sensitive information has occurred.

Education

Administrators and users should be educated in virus defense to help an enterprise effectively protect its systems. Information can be posted on a company's website that shows what the current virus threat is and the number of reports of a virus infection. This allows the individuals in a company to be aware of such threats and help identify any infections. Additional instructions can be provided on how to recognize and handle such infections. To conclude, enterprises should have administrators and users review current policies regarding on a regular basis and provide training in all areas of the virus defense strategy to help prevent or reduce the threat of viruses.

Conclusion

It is vital for an enterprise to protect the integrity of its data in a network from viruses by addressing the threat of malicious code through a virus defense strategy. Virus strategies may differ based on an enterprise's daily activities and need but the importance of protecting its information's integrity from viruses stays the same. This paper provides one example on how to protect a network from viruses by covering three key areas; network level, system level and user level.

---

[1] SourceFire. "Snort" URL: http://www.snort.org/about.html (December 21st, 2003)

[2] Internet Security Systems. "Proventia G & M series" URL: http://www.iss.net/products_services/enterprise_protection (December 21st, 2003)

[3] Worly, Becky. "Protect your handheld device with these antivirus tips". May 21st, 2001. URL: http://www.techtv.com/callforhelp/answerstips/story/0%2C24330%2C3329073%2C00.html (December 25th, 2003)

[4] NAI. "Mcafee Virus Scan and ePolicy Orchestrator". URL: http:\\www.nai.com (December 21st, 2003)

[5] Microsoft Corp. "Microsoft Software Update Service" URL: http://www.microsoft.com/windowsserversystem/sus/default.mspx (December 21st, 2003)

[6] Naraine, Ryan. "Microsoft Security Fightback Includes SUS Overhaul". October 10, 2003. URL: http://www.internetnews.com/dev-news/article.php/3090281 (December 21st, 2003)

[7] Microsoft Corp. "Changes to Functionality in Microsoft Windows XP Service Pack 2". URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=7bd948d7-b791-40b6-8364-685b84158c78&DisplayLang=en (December 21st, 2003)

[8] Deraison, Renaud (founder) "Nessus". URL: http://www.nessus.org/intro.html (December 21st, 2003)

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event