GIAC Security Essentials (GSEC) Practical V1.4b (Option 1)
Rhonda Bramer
May 9, 2003
A comprehensive Malware Strategy for the Global Enterprise Environment:
Battling the Next Generation of Malicious Code

Abstract

According to a reader poll conducted by Information Security, the single greatest threat to security over the next five years is the “super” worm. This new generation of malicious code can target multiple platforms, leverage multiple methods of propagation, disseminate worldwide instantaneously, exploit multiple vulnerabilities and carry severe payloads—from destroying to stealing data. This evolving threat puts organizations at a higher risk of compromise than ever before and requires a strategic revolution from traditional defenses to combat this threat.

The objective of this practical is to provide enterprise organizations with a comprehensive malware protection strategy that is designed to mitigate the potentially dangerous impact of malicious code. This strategy embraces a defense-in-depth approach that combines security technologies with response capabilities to create multiple layers of protection. This paper will describe the various layers that shape the anti-virus architecture and will discuss the technologies and response capabilities necessary to safeguard the confidentiality, integrity and availability of system resources and informational data.

Anti-Virus Architecture

In order to effectively manage virus threats, organizations must first understand the composition of the anti-virus environment and the need for anti-virus protection at each entry point.

The anti-virus architecture can be divided into the following four layers:

- Network Perimeter
- Mail Servers
- (LAN) Servers
- Workstations (includes home and remote users, contractors and vendors)

<u>Network Perimeter</u>

The network perimeter provides connectivity to and from the Internet as well as access to other trusted networks such as clients and/or business partners. Perimeter access points include mail gateways, firewalls and proxy servers. Mail gateways (SMTP) are used to process mail to and from the Internet and are considered to be a primary infection vector. Malicious code written in Active X or Java can also reside on web pages and can enter the network by file downloads or web browsing. Providing anti-virus protection at this layer can guard against threats before they able to infiltrate the enterprise environment.

Even though it is well known that the Internet is the primary distribution channel for malicious code, results from ICSA Labs 8th Annual Computer Virus Prevalence survey revealed that almost all respondents had only limited or no protection at this layer.

Mail Servers

Mail servers are the center of an organizations internal messaging system. Malicious code that propagates via e-mail can clobber the mail severs with thousands of infected mail messages in a very short period of time and cripple this means of communication. By providing protection at this layer, threats that pass through the perimeter can be blocked and stopped. This approach also decreases the risk and reliance of users having the latest signature file updates on their workstations.

(LAN) Servers

Protection at this layer provides security and data integrity for servers that are designed to share files and applications. A virus-infected file on a server can continue to spread to other client systems or other organizations via direct download or network shares. Trapping viruses at the server level before they are replicated and distributed through the environment is another way to limit virus infections and prevent virus disasters.

Workstations

User computers provide numerous pathways for virus infections—from Internet browsing, file downloads, instant messaging, e-mail, peer to peer networks, removable media and storage, etc. This layer is the most vulnerable and can be complicated to manage based on the number and physical location of the machines involved. One of the greater challenges at this level is tracking where an infected system is located and whom it belongs to. Anti-virus protection at this layer is a necessity for any organization.

Technological Defenses

Successfully securing the enterprise environment requires not only the implementation of anti-virus protection for each layer of the architecture but also the augmentation of the solution with additional security technologies. This will provide more granular control and protection against evolving threats present an ongoing risk to the enterprise environment.

Anti-Virus Principles

Anti-Virus protection should be installed and functional at each layer of the architecture—from the perimeter to the workstations--to guard against malcode activity. The deployment of multi-vendor anti-virus packages is another consideration for organizations to examine when trying to ensure the most complete architecture for their environment. Through this type of implementation, organizations can utilize one vendor's anti-virus at the perimeter and mail server layers and implement a different vendor's anti-virus package on the servers and workstations. The allows for the best of breed at each layer and provides for a robust solution that detects and eliminates threats without relying on the capability of any single vendor's suite of products

The anti-virus solution should provide support for multiple operating systems including Windows, Linux, Unix, Netware, etc. Even though most viruses target mostly Microsoft products, according to the Symantec's Internet Security Threat Report there has been in increase in malicious code targeting Linux systems. A good example is the Slapper worm, which exploited an OpenSSL buffer overflow vulnerability to run a shell on a remote computer.

Anti-virus software must intercept malicious code in real time. Inclusion of real time scanning is an effective means of receiving early warning of a virus having entered the environment and to prevent its rapid spread across the network. Organizations often mistakenly choose to disable real time scanning on servers because they feel that it affects system performance. This means that several hours or even days can lapse before an infected server is identified. It can also impede an organizations ability to quickly contain virus outbreaks and minimize system damage and downtime. Similarly, users that have the ability to disable real time monitoring introduce an equally distributed risk to the environment. For example, a user may decide to turn off virus protection to install new software and fail to restore this functionality. Without a method to ensure that anti-virus software is always active, virus protection across the network will degrade as users and administrators alter a well-designed architecture.

File scanning should be set to scan both incoming and outgoing files whereas selecting a single direction provides a limited amount of protection. The limitation of an incoming scan is that it is only performed after the file is closed or flushed to disk and will not prevent the infected file from being opened or executed. This is not recommended because the user if forced to open the infected file before the anti-virus software recognizes the infection. For systems configured only to scan outgoing files, the scan is performed before a file is opened or executed. This is a problematic solution as it will prevent a client from accessing the file and require a restore from known good media.

The strategy must include a hybrid anti-virus solution that adds enforcement and centralized management. Enforcement tools are designed to ensure virus protection is installed, active and that the signatures are up-to-date and active each time a user logs on to the network and also limits the ability to modify the virus software configuration. This ensures that users have limited to no opportunity to undermine what has been carefully crafted to protect them and their resources.

Centralized management provides a mechanism to manage and monitor the landscape of the architecture in real time mode. Without centralization it is difficult to determine the overall network stability as it is unknown and unclear how many systems could be outdated or infected. A lack of capability in this area will force an organization to spend undue time and resources determining just how far a particular virus threat has spread within the environment. The appropriate implementation of centralized management dramatically reduces the number of resources needed to identify and remediate a given issue. This allows for the best use of resources and represents a huge savings in administration and downtime within the organization. An added benefit is the ability to gather and analyze statistical information, identify pockets of architectural weakness and identify repeat offenders.

The anti-virus solution must provide automatic signature protection and the capability to push signature updates throughout the enterprise. Automated signature updates ensure that there is uniformity of the solution across platforms and reduces administration overhead. This functionality provides enhanced protection to the infrastructure from malicious code, faster dissemination of updates and eliminates manual downloading. Without the ability to provide a timely response, an organization is caught flat-footed. This will force them to watch the proliferation of the malware within their environment as they struggle to develop a strategy to clean up the aftermath and return to normal business operations.

Secondary Controls
In addition to defining and selecting anti-virus tools, a secondary control approach will extend the level of protection inherent to the tools by integrating additional security practices into the solution.

Attachment Removal and file Blocking
The removal of attachments and blocking of files prevents certain file types that are used to exploit malicious code from entering the messaging environment. Implementing this functionality proactively prevents a virus from entering the enterprise via external e-mail and greatly decreases the likelihood of viruses spreading. It is very difficult for users to know if an attachment is safe but the filtering functionality will take out the guesswork.

The filtering of inbound attachments containing executables, i.e. exe, vbs, .com, and Jscripts, is a powerful security safeguard. In addition to checking the file type extension, file types can be examined by the analysis of file headers that accurately reveal the content of a file even if the extension has been manipulated. By providing this type of protection, potentially unsafe e-mails will be kept from entering the enterprise environment.

Personal Firewalls
Workstations and portable computers used to access the infrastructure through a remote access or virtual private network (VPN) service should be protected by a personal firewall. Personal firewall protection reduces the risk of compromise and prevents the destruction, disclosure and modification of data on a remote computer. The firewall application must be installed, configured correctly and remain active with periodic updates to maintain the greatest level of security and performance.

Patch Management
Standard patch management processes are a key element in malware strategy. Processes should allow for emergency patch managements of

operating systems and applications. Patch management will provide controls over the deployment and maintenance of upgrades, patches, hot fixes for operating systems and applications. This enables the organization to maintain operational efficiency, overcome security vulnerabilities and maintain stability of the production environment. The consequences of failing to implement patch management process can be severe: critical systems can fail, and security-sensitive systems can be maliciously exploited—both leading to a loss of resources and revenue.

Standard Builds and Baselines

A standard image of common builds should be utilized as systems are built and moved into production. Copies of these images should be kept available for timely restoration of resources that are affected by a virus infection so severely that the anti-virus software is unable to repair the damage. This also provides for consistency throughout the environment and limits exposure of known security risks often overlooked during the creation of custom builds. Standard images of common builds provide a minimum level of acceptable security standards consistent with the organizations system security policy. This will assist in maintaining information security and integrity of systems through the administration of appropriate controls.

Vulnerability Assessments and Management

Vulnerability scanning tools provide a non-intrusive mechanism to assess the enterprise environment and ensure the latest patches have been applied and prevent virus infections from occurring. This capability will identify holes and other weaknesses that could be exploited to gain unauthorized access to proprietary data or launch attacks on other systems. After a virus outbreak, these assessments can also be initiated to determine system stability and as a secondary check to ensure proper remediation. At a minimum, quarterly vulnerability scans are recommended. The results should be presented to the system owners and the mitigation status should be tracked. Management of the vulnerabilities requires the application of countermeasures via standard change control and testing procedures to reduce the risk and the impact of threats to a system. Additionally, this allows for the tracking of known accepted risks.

Intrusion Detection Systems (IDS)

The IDS architecture should consist of network and host-based IDS systems to detect known signature attacks for the network or operating systems that it is protecting or installed on. The IDS sensors analyze traffic on the device(s) and collect information pertinent to an attack. When an alert is generated, specific teams and processes must be executed to handle the response and event handling activities. Even if specific attack signatures do not exist to detect particular viruses, analysis of traffic can be performed based on the vulnerabilities that the malcode would be attempting to exploit.

Mail Usage

Another vector is the unsuspecting user. Users are often naïve and don’t give a second thought to opening an e-mail attachment regardless of the source. Standard mail usage policy should dictate that e-mails with attachments from unknown sources should be deleted without question. It is highly recommended that access to third party e-mail accounts such as Yahoo, Hotmail, MSN, be prohibited. Users often receive virus infections through personal mail accounts that bypass standard anti-virus controls and unintentionally introduce this into enterprise environments.

Internet Usage
The downloading of unauthorized software for use on corporate resources is yet another potential source of malicious code. Users must be aware of the associated risks and disruption that it can cause to the network and internal messaging systems. For example, an electronic card (e-card) application known as FriendsGreeting prompted users to download and run an installer program. When a user clicks on the site and accepts what appears to be a normal default use agreement, the e-card message is then forwarded to every recipient in the user's Outlook address book.

The "FriendGreetings" agreement clearly informs users that, if accepted, e-mail propagation will occur. Although URL blocking can help eliminate users visiting sites like this, an appropriate usage policy should be able to limit this type of exposure. While the FriendsGreetings site did not carry a destructive payload, similar sites could also attempts to access materials that are rated as Confidential for purposes of unsolicited marketing by untrustworthy entities.

Instant Messaging (IM)
This form of communication is vulnerable to attack by IP spoofing and prone to malcode. Use of IM represents a risk to the infrastructure and network. IM message can contain viruses, worms or other forms of malicious code. Unlike e-mail messages, which can be analyzed and stripped of malicious content at the mail server, instant messages can circumvent normal security controls designed to reduce malcode introduction into an environment. An alternative implementation of this technology should provide higher levels of security, allow for secure end-to-end communication, no automatic execution of code and block file transfers.

Response Capability

For day-to-day virus infections and problems, most organizations utilize a multi-tiered methodology. This methodology consists of a first level help desk and escalation points to technical teams and/or field engineers to fix systems for non-technical staff or systems that are located off-site. These technical teams should be well versed in virus infections and ensure proper remediation. However, for large-scale virus attacks, it is recommended that a specialized technical team be prepared to quickly and effectively response to virus attacks. Herein lies the role of the Virus Response Team (VRT). This team complements the existing methodology by monitoring resources of new virus threat and providing virus response.

Though the network engineers and system administrators have traditionally carried out these virus response activities, this is no longer a part time job. It requires the attention of a dedicated staff to ensure this capability is carried out successfully. Virus response must be an integral part of a comprehensive anti-virus strategy and must reach beyond the typical day-to-day issues. The goal is to quickly and effectively respond to new threats and mitigate virus incidents. The size of the team is dependent on the size of the organization. For an enterprise environment, it is recommended that the team is comprised of 6-8 resources. This team may be an extension of an existing Incident Response Team (IRT) or it may be dedicated for virus response and threat management.

The team should be available 24x7 and provide a coordinated delivery of response to constituent organizations. The virus response team serves as the central communication point either via a hotline or pager to receive reports of possible virus attacks. A standard response methodology with processes and procedures to allows for a consistent methodical response. The response methodology defines the six stages of incident handling—preparation, identification, containment, eradication, recovery and post mortem. The post mortem should include an incident report that details the impact, root cause and any preventative actions.

Each of the virus incidents should be tracked in a secure centralized repository. The tool allows for future analysis to be done for each incident handled. Information contained within the tool should support analysis to be done in the following areas: number of infections, cost per incident, repeated trouble areas, non-compliance to anti-virus software standards, budgeting for future organization growth and anti-virus tool evaluation.

Outbreak Support
An organization will benefit from the existing synergistic relationship established between the VRT and extended teams such as a Computer Incident Response, Perimeter Security and Security Administration Teams. These extended teams can help support the mission of the VRT to ensure that virus outbreaks are contained and remediated in the timely manner. This ensures that a minimal impact is felt within the enterprise environment. But provides extended reach to gain control of resources normally outside of the scope of control for the VRT

The VRT will coordinate with the appropriate local, regional and/or global groups, vendors and outside parties and utilize approved processes to assist with response to virus outbreaks. The escalation sequences are controlled and maintained by the VRT but through leveraged support are made more effective for the overall organization. The VRT will work with the extended teams to gather the appropriate information that allows for the identification of the origin and root cause of virus incident as quickly as possible. This information is utilized to create the incident report that is distributed to the appropriate management organizations.

Threat Monitoring
This is proactive response to combat new threat. Understanding the technology that is used is key to being able to successfully assess the risk of a virus threat. Plans need to be available to know how to respond to a

situation located within any particular portion of the anti-virus architecture. The information can be used to assess the threat in order to prevent or mitigate a virus attack. In addition to providing proactive monitoring, a response team must have processes and procedures to synthesize new threat information and provide appropriate guidance to their constituency.

The virus response team should subscribe to multiple alert services that warn of new malcode. It is imperative that organizations are able to react and update defenses within hours of receiving and analyzing the potential affects of the characteristics defined within the malcode. Global organizations are best suited to ensure the most robust implementation of this solution. They are afforded the opportunity to utilize a globally dispersed team and the "Follow-The-Sun" concept. This allows Asia Pacific based resources to notify the remainders of the world in a timely manner rather than allowing the elapsed time of a normal day pass by. Even though this solution will not guarantee that no impact will be felt, organizations can be better prepared for the next "super" worm that is bound to strike.

A validation process should be used to confirm the existence of new malicious code threat. The VRT utilizes standard sources of information when deriving the threat level. The vendors of the implemented anti-virus solution should serve as the primary informational source for this analysis, however, well recognized secondary sources could be taken into account. Reputable sources for additional information include but are not limited to: SANS, CERT, NIPC, AVIEN, Security Focus, and additional anti-virus vendors.

Once the threat is validated, it is processed through a series of risk criteria and metrics to assign an internal risk assessment level. The criterion to determine the threat level includes prevalence, propagation, containment, payload and removal. The resulting value should be reflective of the risk that the threat poses to the infrastructure. There are several risk assessment levels – from high to low, indicative of the risk that the threat represents to the infrastructure and the timeframe during which remediation should be taken.

Conclusion

Successfully securing an enterprise environment against malicious attacks requires a coordinated and centralized defense-in-depth solution. This solution is a careful blending of technology, controls and people. Protection is provided across the enterprise and for each layer of the architecture coupled with an appropriate response capability in order to strengthen the organization's security posture.

Computer viruses will continue to create havoc within global infrastructures if organizations continue to be ignorant to the paradigm shift within the community that is developing the malware. Malware is no longer simple programs that attack from a single injection vector but seek to take advantage of as many avenues of entry as possible. Organizations have failed to learn from history. They are far more prepared to roll the dice and take their chances rather than make the critical investment in an appropriate architecture, which protects their ability to carry out daily business operations. Organizations that make the investment will be able to respond faster and recover with limited impact and long term will be the survivor in their respective industries.

In conclusion, enterprise organizations must weigh their decision for additional protection against the associated costs and the potential consequences of suffering a virus attack and exposing sensitive and proprietary data.

References

Information Security, November 2002, infosec's WORST NIGHTMARES (The 5 past attacks that haunt us, the 5 fears that trouble us.), Ed Skoudis.

Computer virus prevention: a primer, Jan Hruska, Sophos Plc, Oxford, UK
First published: August 2000, Revised: February 2002
http://www.sophos.com/virusinfo/whitepapers/prevention.html

Best practice for multi-tier virus protection
Katherine Carr and David Mitchell, Sophos, Oxford, UK, June 2002
http://www.sophos.com/virusinfo/whitepapers/multi_tier.html

Firms guilty of neglecting remote workers' IT security, reveals Sophos survey, April 29, 2003
http://www.sophos.com/pressoffice/pressrel/uk/20030429survey.html

Symantec Internet Security Threat Report, Volume III, Feb 2003.

Mobiles the target of next virus wave, Kelly Mills, FEBRUARY 04, 2003
http://australianit.news.com.au/articles/0,7204,5920352%5e15321%5e%5enbv%5e15306,00.html

Surviving the Next Virus Attack, *G. Morgan Watkins, Departmental Services*
http://www.utexas.edu/cc/newsletter/jul2000/virus.html

Virus Costs Keep Rising
http://www.vnunet.com/News/1139852

Can firms keep viruses at bay? Madeline Bennett, IT Week,
http://www.vnunet.com/Analysis/1139223

Building "synergistic" AV, May 200s, Peter Tippett,
http://www.infosecuritymag.com/2002/may/synergisticav.shtml

Command and Control: Centralized management solutions provide enterprises with a bird's-eye view of AV defenses, Jack Koziol, May 2002
http://www.infosecuritymag.com/2002/may/commandcontrol.shtml