Global Information Assurance Certification Paper

Effective Virus Defense In Heterogeneous Networks

Jeremy Pickett
April 9, 2001

Introduction

A layered approach to virus protection is a valid conceptual approach for implementing an effective anti-virus policy. However, it does not take into account non-uniform enterprise class networks. There are a number of very serious security implications that a heterogeneous environment produces that a layered approach does a poor job of handling. These include (but are not limited to) lack of support for OS's that may be running in that environment; inadequate knowledge of the topology of the enterprise network; inadequate tools with which to remotely administer workstations; and informal security procedures that can put anti-virus software in a vulnerable position. What is needed is a formalized policy and process in which you have determined what your needs are, how you are going to implement this solution without compromising stability, and how you are going to continually test the solution to make sure that it still fits your needs. I would like to propose a Procedural Approach to be the most effective defense against malicious code.

The inherent difficulty in dealing with virus outbreaks originates from several sources. More often than not, a virus exploits a valid feature in a program or operating system. This issue has recently gained a high degree of visibility, since most of the more devastating outbreaks have used features such as Windows Scripting and Macros to propagate (i.e., Melissa, Anna Kournikova, etc). The second source comes from either a lack of a policy regarding OS and application patching, or the ineffective implementation of that policy. This is usually the result of an administrator not having a clear picture of his/her network. If they do not know about every installation of Linux, then how will they have control over the patching potentially dangerous security holes? Recently we have seen several viruses that have taken advantage of flaws in certain versions of BIND and are able to gain root access, then search for more vulnerable boxes with exploitable versions of BIND running on them. The third, and perhaps most frustrating, is that it is almost impossible to predict what kinds of viruses will become large threats, and therefore anti-virus companies are forced to *react* to a new virus. It is particularly painful when an enterprise implements an anti-virus solution, to find that a virus made it through their defenses undetected. There are usually measures implemented by various vendors (commonly called heuristics) that claim to be able to detect viruses that have not been discovered yet, but this type of scanning is fairly easy to thwart.

Virus prevention is not just installing a piece of software on your machines and hoping for the best. This is a dangerous view, because like all aspects of security, virus protection is a process that must constantly be monitored, checked, and reviewed. Virus prevention is a multi-step process which insures the feasibility, availability, and integrity of the infrastructure. It should also be an integral part of an enterprise's total security architecture. With that being said, let's look at the Procedural Approach to Virus Protection.

Step One: Know thy Network

C.G. Jung said, "Know thy self", and this is very close to the mantra that one needs to adopt to implement an effective anti-virus policy. An undocumented (or poorly documented, or incorrectly documented) network will be a haven for viruses. The key points specifically are:

1. How many and what kinds of mail servers are you running.
2. How many and what kind of file servers are you running.
3. Where are your slowest network links, both WAN and LAN.
4. How do remote users connect and gain access to network resources.
5. What process exists to verify software is installed and running on servers and workstations.
6. What rights do users have to their own machines.
7. What operating systems exist in your network.

The key issues these questions will help to address are:

1. What anti-virus vendor can meet my specific needs in regards to management, operating system support, and flexibility.
2. What existing resources can I leverage to make my anti-virus investment more effective (For instance login scripts, SMS, ZenWorks, or Tivoli for remote installation of the software).
3. What options do I have for distribution of pattern files/definitions/dats to my users. Does the built in distribution methods fit my needs?

Not all virus companies have support for all OS's. Generally the impetus behind not developing these products is that either the market is too small or a threat for that OS has not positively been identified. This can be dangerous for some enterprise class customers, however. While it is true that most viruses only attack Windows-based systems, it is also true that any OS that interacts with a Windows system can propagate Windows-based viruses (such as Linux Samba shares propagating macro viruses and so on).

Another consideration is what level of management you need. Management, when referring to anti-virus software, usually refers to reporting of events from clients to a central console, centralized administration of pattern files/definitions/dats to clients, and the ability to initiate events on the client from a centralized location. Almost every major anti-virus vendor has an Enterprise version of their software available, usually with some level of manageability. This may or may not fit your enterprise.

Other products and policies of your security architecture can have a positive impact on your anti-virus protection. These are things like policies on attachments being sent over the corporate email system, rights the users have to their boxes, maintenance done to users' machines, and especially policies regarding remote users. The same care that is taken in administering local users needs to take place with remote users. However, the process is usually a bit different, since they have different needs arising from their environment. With slow connections and less ability to be monitored, mobile users are a challenge for IT administrators. Slow connections make it difficult to push out new versions of anti-virus software and patterns/definitions/dats. In addition to that, it makes it more difficult to use administrative tools to monitor and track these systems. If the user has administrative rights to the box, a level of trust has to exist that they will not turn off the anti-virus service, and thus open themselves up to infection. Some features that you may look for in an anti-virus solution are automatic updates from both a centralized location in your LAN, and also from an Internet source. A thin client can make the initial distribution of the software less painful for both the remote user and the administrator. And some kind of micro pattern/definition/dat so that updates occur as fast as possible.

Step Two: Develop Strong Anti-Virus Policies

This is another critical step. What you want to accomplish here is set the standard for what parts of the overall virus solution you want to implement (email gateway protection, direct mail server protection, desktop protection, anti-virus API's for in-house applications), the availability of the solution (and measures to insure that availability), the most effective way of applying updates to the product, how to audit your solution to insure integrity, and what to do when you have a virus outbreak.

There are several things that need to be accounted for when deploying to a workstation level. All of these items listed should be part of your anti-virus policy to make sure that all machines as defined by your needs are covered, and the anti-virus solution has the highest availability and effectiveness.

1. How are you going to get the software to the machines? Leveraging an existing technique is highly desirable here. If you have something like login scripts, SMS, ZenWorks, or Tivoli, it will greatly speed up distribution. There also needs to be a plan for getting the software on remote machines. If your software choice has a thin client version, this will probably make things go a lot easier. If not, you will have to evaluate if a network install process is right for you.
2. How are you going to make sure that your users cannot disable or remove the anti-virus software. If your security policy included limiting access to administrative accounts, then this issue has been taken care of. If not, either you will want to look at implementing a policy such as this or create a 'paper policy' that all employees must abide by. If the virus scanning software is turned off, then you have an unguarded point of entry that can be compromised.
3. How are you going to update your clients. Most products have built-in update features, but these do not always fit in every environment. It is imperative that they are tested and a solid plan is built for how to update your clients, how to check they are updated, and what to do if it stops working.

If one has their policies set up so that they are implemented, audited, and updated, then generally dealing with a virus outbreak will not be a catastrophe. It is when one of the afore mentioned policies is ineffective that outbreaks become extremely serious. For instance, if a VBS virus were to emerge and you had implemented an SMTP Gateway product, it could be caught right there. However, if you did not have a tested update policy on the product and it did not receive the pattern file/definition/dat, then there could be serious trouble. Another example: someone brings his or her laptop to work. They attach to the network and log in. However, when they were at home they disabled the anti-virus service, since they believed it was slowing down their performance. They then received an email from their Hotmail account that contained a virus that can propagate via network shares. If it were a virus like Funlove, then it would search all network shares and infect the computers that it found. This could have been

prevented had there been a policy that would have prevented the user from disabling the virus protection. That policy could have been technical (like not having enough rights to terminate the service) or it could have been a strong formal written policy. Either way, because that policy was defeated it opened up the entire organization to an attack from this virus.

Step Three: Test and Audit

This applies not only to the anti-virus software, but also to your security architecture (because they are all one and the same, right?). The policies that were set up in Part Two need to be tested. This can be accomplished without releasing a wild virus on to your network. Simple questions like, "Are there any new workstations in our environment, and do they have anti-virus software on them?" is a good start. A good test for an administrator would be to see how fast they can check pattern file/definition/dat versions on all systems in their enterprise. If there is more than one anti-virus administrator, how often do they meet and discuss their strategies? Also, real virus outbreak data is vital to making sure that your organization is running well. What happened in the last outbreak? How long did it take us to get back up and running?

A tool that will be invaluable at this stage is the EICAR test string found at www.eicar.org. Every major anti-virus vendor supports this string. Although it is not a virus, if an anti-virus scanner finds this string, it will treat it as a virus. You can use it to send through your email system to make sure that it is protected, or to check desktop machines, and so on. This tool can be used to verify that the scanning engine or services are enabled and running, that reporting features are working, that a virus will be stopped where you think it will be stopped, and the different points of entry that are in your enterprise.

Network monitoring software may also be very handy. Knowing how much data is going between clients and the management console could impact your decision on how to implement your solution. If the management console were to be pushing5 megabyte updates to each client every week, this might not be a scalable solution for a large enterprise without a lot of network resources.

This takes us back to step one. Now that we have documented our policies and procedures, do they still work as the enterprise changes? If the WAN infrastructure gets a dramatic upgrade, it might be that there will be more efficient ways of doing tasks such as updating the software, distributing it to new workstations, and auditing the results. It is important to note that there is no one way that an anti-virus solution can be implemented, so like the rest of your security architecture it must be monitored, maintained, and evaluated.

Conclusion

The rise of computer viruses as one of the most reported about network security issues has lead to a lot of misinformation about the subject. There is no magic bullet, no perfect solution, and no software that will let us peer into the mind of a virus writer to tell us what he will do next.

Multiple levels of protection are vital to keeping a company secure from malicious code. However, what is even more important is having the policies and procedures documented from start to finish on how to keep this infrastructure running in peak performance. These policies need not be overly elaborate, but they need to address the issue of keeping known malicious code out of your enterprise, preventing undiscovered code from compromising your enterprise, and keep your network staff aware of what is happening.

References

i. Symantec. "SARC Writeup – VBS.SST@mm." 28 Feb. 2001. http://www.sarc.com/avcenter/venc/data/vbs.sst@mm.html (8 April 2001).

ii. Symantec. "SARC Writeup – Linux.adore.worm." 6 April 2001. http://www.sarc.com/avcenter/venc/data/linux.adore.worm.html (8 April 2001).

iii. Dunham, Ken. "[K] Tells Us How Easy It Is To Beat AV Scanners With VBSWG 2.0." 14 March 2001. http://www.securityportal.com/articles/vbswg20010314.html (8 April 2001).

iv. Trend Micro. "Trend Micro Virus Encyclopedia." http://www.trend.com/vinfo/virusencyclo/default5.asp?VName=PE_FUNLOVE.4099 (8 April 2001).

v. Kaufman, Oren. "Keeping Worms out of your PC." 4 April 2001. http://www.zdnet.com/zdnn/stories/comment/0,5859,2704658,00.html (8 April 2001).

vi. Eicar.org. "Anti-virus Test File."
http://www.eicar.org/anti_virus_test_file.htm (9 April 2001)

Last Updated: May 30th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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 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
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
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
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
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
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event