Global Information Assurance Certification Paper

December 6, 2001
Shawn Wyman
GSEC Practical

Anti-Virus Strategy in a public K-12 Educational Environment

Introduction

In today's private industry, it is imperative to have virus protection on all of the organizations electronic resources. Corruption of data means loss of revenue and possibly your job.

Unlike private industry, public K-12 educational institutions rely heavily on government funding and community fund raising. This means that many K-12 educational institutions have very limited budgets that restrict their ability to use the latest and greatest in virus protection technology. This also means less money to hire enough qualified resources. School boards are often left with hiring temps, contractors, and even parent volunteers to help maintain sometimes very complex networks.

School boards are constantly acquiring new workstations that are being connected to the network. IT staff does not grow proportionately with this increase and are faced with more network nodes to monitor with no increase in resources. In comparison to private industry, educational institutions have a much higher percentage of users who are purposely trying to disrupt their institutions electronic services.

As well, the repercussions that a student faces are typically not as severe as what would happen to private industry employee. If an employee were caught infecting a system with a virus, their employment would almost certainly be terminated. The typical consequence a K-12 student would face for infecting a computer system with a virus would be loss of computer access privileges. Students also have a large amount of time that they can dedicate to finding holes and vulnerabilities in their school networks. School network admins are usually too busy just trying to maintaining their environment and deal with every day problems.

What an educational institution requires is a cost-effective and centrally managed "defense-in-depth" approach to virus protection. The days of installing anti-virus software on the desktop and believing that all systems are adequately protected have long disappeared. Educational institutions are always looking to expand student learning by introducing new technology. Education and security do not always go hand in hand resulting in school administrators who do not want to inhibit student learning with security restrictions.

School environments use many different operating systems for educational purposes.

Although this is important for it's educational value, it becomes increasingly difficult to make sure there is adequate anti-virus protection on all operating systems.
Although most of the viruses that are discussed in mainstream media are for Microsoft's Windows platform, all operating systems are vulnerable to virus infection if not properly protected. Many non-Microsoft platforms include Windows emulators and Microsoft Office applications that can be just as vulnerable.

What needs virus protection?

There are many different ways that viruses can infiltrate computer systems today:

- Floppy Disk and other removable media
- Email
- Internet downloading
- P2P file sharing programs
- IRC and Instant Messaging
- Wireless devices and Hand Held Devices
- Network shares
- Improperly configured applications and operating systems
- Improperly secured operating systems

How can we protect against all of these methods of infection?

Traditional methods of virus protection usually involved only having some sort of desktop anti-virus software installed on the workstation or server.
In an educational environment there is the risk that new, re-formatted, re-imaged or donated computers will not have up to date, properly configured anti-virus software.

Desktop protection is obviously not the only solution for an educational institution. Some workstations may find their way onto the network without approval. For instance someone may bring in a donated machine, or perhaps his or her home computer. Some computers may have their anti-virus software corrupted, which causes it to stop functioning. Students will even try to purposely disable desktop anti-virus software. Staff might also try to disable desktop software if they believe it is interfering with their other applications or giving performance problems. Even if the desktop component has password protected the disabling and uninstalling components, there are always ways a user can find to disable applications.
This means you cannot trust the anti-virus software on the desktop 100% of the time and other anti-virus measures are needed.
In order to ensure confidentiality, integrity and availability of all electronic resources, a "defense-in-depth" approach is needed when deciding on how and where to deploy anti-virus products.

- **Security Policy**
  The most important aspect when designing an anti-virus strategy is to ensure that it fits into your corporate security policy. If you do not have a security policy, then your priority should be in creating one and getting senior management to endorse it. There will be many obstacles to overcome when implementing an anti-virus strategy. Technical issues, lack of resources, and uncooperative users are just to name a few. Performing a risk assessment will identify the organizations assets, threats, and vulnerabilities. Risk assessment will help drive the creation of a security policy. A security policy provides the framework from which all IT related decisions are made. With a corporate security policy you and your institution will better understand what needs protection, and why it needs to be protected. From the security policy you will be able to successfully develop the architecture required to meet the goals of the security policy.

- **Desktop**
  All desktops must have up to date and properly configured anti-virus software. Desktop protection is the last line of defense against viruses, and must be protected at all times. To help ensure this, the anti-virus software must be able to update its pattern, engine and program files automatically with little or no user intervention. Having only guidelines or written policy that users should keep their anti-virus program up to date will fail every time. Centrally monitored and maintained desktop anti-virus protection will ensure that all computers are up to date and that users will be alerted to any virus activity found. Users will also try to uninstall desktop anti-virus programs if they feel that it is interfering with their other applications or if it is too resource intensive. A good anti-virus product will have a small footprint.

- **Servers and Operating Systems Vulnerabilities**
  Virus developers today are always looking for new ways to infect systems. In reality there are only two ways that a computer is compromised. Either the computer system has an application that has vulnerability in its code, or the operating system has not been properly secured. In recent news, Microsoft's IIS was a target for having a vulnerability in it's code and this vulnerability was exploited by viruses such as Code Red and Nimda. Protect all file and application servers. Make sure that all shared folders and files are properly secured to prevent unauthorized users from having write access. Perform vulnerability scans on all servers to ensure that no known operating system or application level vulnerability exists. Code Red and Nimda viruses both exploited known operating system and application vulnerabilities. Subscribe to security email lists, anti-virus lists, and frequent security pages, such as http://www.ciac.org/ciac/, for the latest on system vulnerabilities and security news.

- **Floppy Disk and other Removable Media**

This is still a very popular way of infecting computer systems. It is very common for staff and students to take schoolwork home on a floppy disk for use on their home computers, which may not have up to date anti-virus software. It is very common to see floppy disks with boot sector viruses or documents infected with macro viruses. The only line of defense against a floppy disk is properly configured and updated desktop anti-virus software. Some school sites have disabled floppy disk drives or even removed them entirely to prevent infection from floppy disks.

- **Email and SMTP**
  This is still the most popular method of infection today. With high-speed Internet access and instantaneous email messaging, a virus can quickly spread to hundreds or even thousands of users in a matter of seconds. Since many of today's email viruses are in the form of executable attachments, a corporate policy should consider blocking all executable attachments. .EXE, .SCR, .VBS, .COM, .BAT, .JS, .PIF, .SHS, .PIF, .CMD are just a few extensions that are commonly used by viruses and should be stripped from both incoming and outgoing emails. Blocking virus emails with known subject lines is also recommended, although newer email viruses have dynamically changing subject and content, so this is not a fool proof method. Having users configure their email readers to not automatically open attachments.
  Encouraging the use of Rich Text Format (RTF) instead of HTML that can contain malicious applets and scripts would be beneficial. Scanning of all SMTP traffic at the gateway would be another option. As well your gateway should only let through SMTP traffic from your email servers. This will prevent users from setting up their own POP email clients to access their home email, which could have viruses.
  Scan all corporate inboxes, both inbound and outbound for viruses. Block email spamming viruses to prevent flooding email servers. As well, the corporate policy should include stripping all executable attachments, as well as disabling HTML emails that can include malicious scripts and applets.

- **HTTP and FTP**
  Two very common methods for virus infection are by downloading from the Internet. Users can unknowingly download virus-infected executables, or knowingly download virus creation toolkits. Gateway HTTP and FTP scanners will help in preventing web and ftp virus downloads.
  Real-time virus detection and cleaning for all HTTP, FTP, and even SMTP Internet traffic at the gateway will help to prevent infection to workstations that may have their desktop anti-virus disabled. Look for transparent gateway virus filtering. Anti-Virus products that rely on client side configurations will not work in an educational environment. Both staff and students will change client configurations to circumvent anti-virus scanners for various reasons.
  Consider including behavior scanning for malicious applets and scripts that will detect new and unknown virus strains. This will help protect against new and unknown viruses that do not have a definition file yet created by anti-virus products. Content filtering at the gateway for inappropriate web sites that contains viruses or virus

creation tools will help prevent users from accidentally or intentionally infecting their systems.

- **Internet Web Content Filtering**
  The Internet is obviously a wealth of information, both educational and non-educational. Unfortunately it is sometimes difficult for Education institutions to distinguish between the two.
  Having a transparent content-filtering proxy server is a step that helps to prevent users from accessing virus creation sites, hacker sites, as well as other inappropriate sites that may contain viruses.
  Although content-filtering proxies do not prevent virus infection, they help prevent users from getting to inappropriate sites that may contain viruses.
  Filtering systems cannot block all of the thousands of new web sites being created every day, but they do help protect against the majority of the known problem sites.

- **IDS & Firewalls**
  Setting up internal firewalls to help segregate different areas from exposure to others will also help prevent to spread of virus infections. Newer Intrusion Detection Systems (IDS) also have the ability to use signature plug-ins for viruses so they can detect, alert, and stop viruses from spreading across the wire.

- **P2P**
  Peer-to-Peer share-applications such as Napster, Morpheus, Limewire, AudioGalaxy and BearShare (just to name a few) are becoming exponentially popular for users to share applications and files. Some of these products use static ports that can easily be blocked at the gateway firewall. Some, like Napster, have dynamic port assignments, which make it impossible to port block on the Firewall. Some Firewalls can detect the traffic patterns of P2P applications and will deny this type of network traffic.

- **IRC and Instant Messaging**
  Similar to P2P applications, Instant Messaging like ICQ, AIM, Microsoft Instant Messenger and Internet Relay Chat programs mIRC are other ways that users can transmit applications and files across the Internet. Viruses can be downloaded using these applications, and if they are not configured correctly may also receive file transfers automatically. Not only can files be downloaded but also some virus's install Trojan exploits on these programs, which allow back door access to malicious users.

- **Wireless**
  This is a new potential for virus infection. The use of wireless technology is increasing exponentially in educational institutions because it is a cheaper alternative to traditional physical wiring. Without a properly secured wireless network, there is the possibility that an unauthorized malicious user could connect to the network with the use of a laptop and wireless NIC. To prevent against this, all wireless installations

should have proper security in place. This includes properly configured Wired Equivalent Protection (WEP), MAC based address filtering, RADIUS Authentication, as well as the using Virtual Private Networks (VPN) and firewalls to secure the wireless network connection from the physical network.

- **PDA and Hand Held Devices**
  Personal Digital Assistant (PDA) or hand held devices which are wireless or non wireless, should still have anti-virus software protection installed on them. This will keep them protected when they sync up with other PDA devices and other workstations that may not have adequate anti-virus installed on them. There are some PDA viruses that can spread to computer systems and networks until it is uploaded to a PDA device where it executes its payload. PDA devices can also transmit viruses through infrared. Something as innocent as exchanging business cards could lead to the spread of a virus.

- **VPN and Dial Up**
  More and more users want to work from home. Teachers and students are no exception. You must ensure that their home computers and all corporate laptop computers are properly equipped with anti-virus software, as well as other applications like intrusion detection and personal firewalls. With affordable high speed Internet for home users, it becomes very easy for home-based systems to become infected with viruses. Proper virus protection is very important for VPN and Dial Up clients, since most VPN's tunnel though gateway firewalls and might not be subject to gateway anti-virus scanners.

- **Network Shares**
  In educational institutions it is common for departments and schools to want to share their information to others. Unfortunately this can lead to improperly secured network shares. It would be very easy to accidentally share out an entire hard drive to all users. Open network shares are becoming targets for today's newer viruses such as the Nimda virus. Nimda scans entire networks looking for open network shares and will infect them with dozens of virus files if those workstations are not properly protected. Enforce a security policy that only secured server shares are to be used and that no workstation shares are to be created. Perform routine audits looking for workstations that insecurely share out folders.

- **New and Unknown Viruses**
  Even if your anti-virus system is up to date with the latest definition files and engine, it could still be vulnerable to a new virus that has never been seen before. Some viruses are compressed using various types of packers that some anti-virus software won't recognize and thus lets it pass through without being detected. New types of defense are programs that do behavior monitoring and blocking. Any activity that is considered malicious will be blocked. This is very useful in fighting new, quickly spreading viruses (I Love You, Code Red and Nimda are good examples) that anti-

virus vendors have not had a chance to create a definition or pattern file for.

- **Staff for Handling Viruses**
  It is all good to have virus protection on all systems and to have centralized management, but when a virus does get into the system, you need to be able to have someone action it. It's the same principle as server event logs and firewall logs, if nobody actions the alerts, then what's the point of having them?
  When a virus alert does hit the system, there needs to be policy and procedures in place for people to action those incidents.

When you get a Virus

Be prepared. It is not "if" you get a virus, but "when". Even if your company has the latest anti-virus software running at the gateway, email servers, file and app servers, and on all the desktops, eventually you will still get a virus infection. You need to be prepared for a virus outbreak.
Without knowing exactly what to do precious time is wasted and viruses can quickly spread to critical systems.
Upper management support for handling all emergency incidents, including viruses, is a definite must. Without support from the top it will be extremely difficult to get schools and other departments to cooperate and work together on bringing the emergency under control. All institutions including educational must have a corporate computer security policy that discusses emergency handling procedures that include virus defense.
Developing a Computer Emergency Response Team (CERT) is critical to ensure that any emergency including a virus outbreak is handled quickly and accurately. There are several phases a good CERT team must follow, and although it is out of scope in this paper, it is still important to highlight the main points of a good CERT plan:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow-up.

The most important phase is preparation. Selecting the incident handling team, developing an emergency communication plan, and conducting training exercises are all critical to properly prepare your organization for a computer emergency. This will help everyone be prepared for when a virus outbreak occurs.

Choosing the Right Anti-Virus Application

For an educational institution the costs can be tremendous when considering an anti-virus strategy. There are a few things that can help leverage your decision when choosing the right anti-virus application.

- **Total Cost of Ownership**
  The cost of the investment is usually the primary concern. However, total cost of ownership (TCO) must be acknowledged when choosing the product. The "sticker price" is rarely the total cost of the product.

- **Educational Discount**
  Most vendors have educational discounts; make sure that when you are doing a request for purchase that you are not getting the retail price. Educational discounts are usually quite significant.

- **Licensing**
  In an educational environment, the staff and user population is generally the same from year to year with only minor fluctuations. However, the numbers of networked computers in educational institutions increase dramatically each year. If an anti-virus vendor only has workstation/node based licensing, then your costs will also dramatically increase every year. Try to negotiate a user based licensing scheme. It not only will be significantly less expensive in the long run but also much easier to manage. It is often very difficult to get an accurate count of workstations in a computer institution since many computers are donations, brought in from fund raising events or moved to different schools. Staff and student user counts are much easier to track through Human Resources and student record information. Be sure to negotiate licensing for home users as well. It is much easier to get teachers and students to use anti-virus products at home if the school board can pay for the licensing costs.

- **Vendor Support**
  You want to make sure that the application you choose has the vendor support you will need. If they are a small organization, chances are that they will not be there for you when there is a virus outbreak. You need to be sure that you have dedicated resources from the vendor who will be available, either in person or on the phone, to assist when there is a virus incident. They should also have references for other educational institutions or similar sized organizations for which they support. If their main customer group is home users or private companies, then they will not have the background on how educational institutions work and will not be of very much help if they are required to assist in the anti-virus enterprise design.

- **Operating Systems**
  Typical educational institutions use multiple operating systems from Microsoft to Apple to the various flavors of Unix. No operating system is immune to viruses. Microsoft operating systems and applications are well known for their virus incidents,

but they are not the only ones susceptible to virus infection. All operating systems can contract computer viruses if they are not properly secured. Your anti-virus application should be able to support 90% of all of your supported operating system platforms. There is some debate that separate anti-virus programs helps give another layer of defense; if a virus slips through one AV application, the other may catch it. However, choosing different anti-virus applications will lead to larger licensing and operating costs. Management of separate applications will become more difficult. If possible try to limit it to one or two different anti-virus applications.

- **Central Management**
  This is the critical component for an educational institution. With limited staff resources to manage the anti-virus software it is imperative that there is a central management built into the anti-virus products.
  A typical educational institution may consist of hundreds of different school locations. Each school may or may not have adequate technical staff to help out with installations and monitoring. Thus central management is a pre-requisite to an educational anti-virus solution.
  The AV application should be able to monitor and configure all aspects of your anti-virus applications, regardless of the platform or physical location.
  It should also provide comprehensive analysis and statistics through custom reports. Remote and secure installation to clients, automatic definition and engine updating, alerting to virus infection and outbreaks are also critical for successful central management. Without a centralized management console it would be virtually impossible to be able to tell if all components were protected.
  Typically in an un-managed scenario all workstations and servers would have anti-virus software installed through a long and tedious manual process. However, it would not be long before users either disabled the software, uninstalled the software, or the software stops updating for other reasons. In an unmanaged environment it is impossible to tell which computers are protected.

Education

This is by far the most important element in protecting the environment from viruses. All users must be educated on the dangers of viruses, how to help protect the environment from viruses and what the consequences are for those who purposely infect systems with a virus.
All users must know that they are part of the solution; all of the virus protection in place will not succeed if the users do not help.

Suggestions to raise user awareness on Viruses

- Develop a corporate computer security policy that includes anti-virus policies. Make this policy easily available and easy to understand for all users.
- Intranet web site containing corporate security policy and information on how to

stay virus free and who to contact for questions, concerns or virus incidents.

- Annual meetings with management and principals will help keep them aware of the dangers and how to avoid infection.
- Monthly meetings with new staff and teachers will help enforce this at the beginning of their career.
- An annual "Security Awareness" day to hold demonstrations and information sessions about the dangers of viruses and how to spot a virus.
- Monthly bulletins about people who have helped prevent the spread of virus infections.
- Emails to all users about new viruses and how to protect home computers.
- Monthly reports to management and principals on how many virus incidents were detected, how many were prevented, and how many workstations were actually infected.
- Inform all users of new, high risk Viruses so that they know what to be watchful for and how they can protect their work and home computers from infection
- Contact the user when there is a virus alert on their system. Even if the anti-virus cleaned the infected file, if they have been made aware that there was an incident, they will be more cautious in their computer activity in the future.

Virus protection in a K-12 educational environment is difficult, but not impossible to properly maintain. With user education, security policies and procedures and the right anti-virus tools in place, you will drastically reduce your chances of virus infection. When a virus does infect your systems, you will be prepared with a quick, accurate and measured response.

References

The SANS Institute, Computer Security Incident Handling Step By Step, Version 1.5
Author: Stephen Northcutt

TruSecure, Information Security Magazine, April 2001 Issue
Airborn Viruses, page 80

TruSecure, Information Security Magazine, February 2001 Issue
AV Alternative – Behavior Blockers, page 52

TruSecure, Information Security Magazine, May 2001 Issue
VPN – The Good, the Bad & the Ugly, page 48

Computer Incident Advisory Capability, "Security Advisory"
http://www.ciac.org/ciac/

University of Florida “Information Technology Security Awareness”, September 26th, 2001
http://www.itsa.ufl.edu

SecurityFocus.com, "BugTraq and SecurityFocus Mailing Lists"
http://www.securityfocus.com

Microsoft Corporation , "Microsoft Security "
http://www.microsoft.com/security/

Trend NeatSuite, “The comprehensive virus protection suite for the enterprise”
http://www.antivirus.com/products/neatsuite/

Symantec, “Enterprise Security”
http://enterprisesecurity.symantec.com/content/productlink.cfm#0

Finjan Software, “SurfinGate”
http://www.finjan.com/products_home.cfm

McAfee, “Gateway WebShield Appliances”
http://www.mcafeeb2b.com/products/internet-gateway-protection.asp

N2H2, “Bess® Internet Filtering Service”
http://www.n2h2.com/products/g2100/index.php

ISS RealSecure, “Intrusion Detection”:
http://www.iss.net/securing_e-business/security_products/intrusion_detection/

CheckPoint, “FireWall-1 Content Security”
http://www.checkpoint.com/products/security/firewall-1_security.html

TrendMicro AppletTrap, “Comprehensive Malicious Code Solution for the Enterprise”
http://www.antivirus.com/products/isat/

Aladdin’s eSafe, “eSafe Gateway”
http://www.esafe.com/esafe/gateway/index.asp?cf=tl

TrendMicro, “Wireless PDA Protection”
http://www.antivirus.com/free_tools/wireless/

PCWorld.COM, “Viruses May Be Ready to Go Mobile”, June 08, 2001
http://www.pcworld.com/news/article/0,aid,52166,00.asp

Last Updated: May 29th, 2017

Upcoming Training

SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
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 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
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 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
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