GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

A Practical Implementation of Norton Antivirus 7.6 Corporate Edition

By
Jeff McCarthy
12 November 2003
GSEC
Version 1.4b
Option 2

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A practical implementation of Norton Antivirus 7.6 Corporate Edition
- Abstract -

This paper describes the process which Company X followed to upgrade their antivirus environment. I will briefly touch on how Company X successfully implemented Norton Antivirus 7.6 Corporate Edition on all of the laptops, servers, and workstations throughout the network. This paper defines what the minimum requirements were to successfully implement Norton Antivirus 7.6 Corporate Edition in the Company X environment, and what prerequisites had to be completed before the upgrade.

This paper will review the Norton Antivirus for Exchange configuration, and how Norton Antivirus for Exchange has significantly reduced the number of virus alerts received on all the Windows platforms. I will describe the configuration of the centrally managed antivirus solution, touching on the policies, and I will list the various responsibilities identified for monitoring, responding, and maintaining the system at Company X. I will provide a few virus infection examples Company X had during the antivirus upgrade process; and I will list some examples of how Norton Antivirus has helped reduce the spread of computer viruses, worms, and Trojan horses in the environment. Finally I will discuss what other security changes Company X implemented to reduce the risk of Malware in the environment.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Background

Company X was running Norton Antivirus 4.x and 5.x on all laptops, servers, and workstations throughout the organization. Company X relied on the users to call the Support Center to report a virus infection on their laptop or workstation. A few users would call the Support Center when they had a virus alert, but most did not. Some tried to fix the problem themselves, ignore the virus alerts, or simply disable the auto-protection features of Norton Antivirus. The other significant problem was that Company X relied on the users to update their virus definitions, which most users did not bother to perform.

My role was to take ownership of the antivirus system back in 1999; and mold it into a centrally managed antivirus system. I set up a process where Company X would distribute monthly emails to all users reminding them to update their virus definitions; we even went so far as to state it was a requirement to update their virus definitions. We embedded object links in the emails directing the users to which object to click on to install the live updates. These object links were named for each specific network location and had an embedded batch file. The batch file ran the executable containing the virus definitions, which were installed on their local print share workstation. Company X typically designated an individual workstation to host print queues for printing to local network printers. Again, we relied on the users to execute this process. We also configured another batch file for the dial in users to run. This batch file copied the diskette versions of live update to their local hard drive and then executed the updates. It was surprising how many people actually updated their virus definitions, but there were always users who did not, and if they had problems they did not bother to report them.

The Problem

Malware infections were a problem from the late 1990's through 2001 with Company X. "Malware is a generic term that refers to software that was written with malicious intent and performs it actions without the user's permission."[1] Company X had several cases of desktop users infecting their computers with infected diskettes and CDs. These cases were rarely reported to the Support Center and a few caused problems on file servers and other desktops. Company X relied on monthly antivirus definition updates for the servers, workstations, and laptops.

The most significant problem Company X needed to control was the spread of email borne Malware. Company X had installed Norton Antivirus for Exchange 2.11 on the exchange server, but we had not effectively detected any viruses without an updated signature on the Exchange server. We assumed Norton Antivirus for Exchange would stop all email transported malware with the Bloodhound technology.
1

[1] "SANS Security Essentials with CISSP CBK" version 2.1 volume 2, page 1056

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Company X also had users exploiting the firewall configuration, using web email to inadvertently transport computer viruses, worms, and Trojan horses into the network. Malware infections were a frequent occurrence for many businesses and Company X was no exception. Company X needed a centralized antivirus management system to combat virus invasions on the servers, workstations, laptops, and Exchange server.

Antivirus Software Upgrade Selection

In March 2001, Company X investigated the various antivirus solutions on the market to determine if the timing was right to switch from a Norton Antivirus 4.x/5.x install base to a competitor's solution or to renew the licenses with Symantec and upgrade to Norton Antivirus 7.51 Corporate Edition. We took a look at two of the major competitors (Computer Associates – Inoculan 4.0, and Network Associates – McAfee VirusScan 5.x) to determine what advantages would be gained by migrating to their enterprise or corporate solutions. Neither one of these companies had a solution that was significantly different than Symantec's. They all required an 8 – 15 mbyte client installation set to be pushed or installed across the WAN to the client server, workstation, or laptops. If Company X were to migrate to one of these two solutions we would have to manually uninstall Norton Antivirus 4.x/5.x from every server, workstation, and laptop prior to installing the antivirus client from either Computer Associates or Network Associates.

While Symantec's upgrade installation process from Norton AV 4.x/5.x to Norton Antivirus 7.51 Corporate Edition (CE) was completely automated, the two competitor's solutions would not uninstall the old version of Norton AV 4.x/5.x, and required a reboot. The installation of Norton Antivirus 7.51 CE would simply stop the Norton AV 4.x/5.x processes, and upgrade the client to version Norton Antivirus 7.51 CE. Plus, no reboot was required for the client install. The obstacle of manually removing Norton AV 4.x/5.x, rebooting, and installing one of the competitor's solutions was too significant of a change to justify switching from Symantec's solution; besides Symantec includes Norton Antivirus for Exchange Server with enterprise licensing agreements.

Configuration planning

After the decision was made to stay with Symantec Company X had to design a centrally managed, but distributed system. This new antivirus solution would have little impact on the Wide Area Network (WAN) links, while still providing centralized management of the antivirus clients.

Company X had 1100 plus workstations and laptops spread across 30 plus remote sites to upgrade, and Company X wanted to accomplish the installation and distributed management from the local Area Network (LAN) to avoid pushing 12 mbytes per workstation across the WAN. Company X also had about 65

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

servers to upgrade. The 30-plus remote sites are connected via a frame relay network with connection speeds of 128kbps to 256kbps to the central site. We had to find a solution to upgrade, manage, monitor, and receive alerts from remote clients without impacting the business processes running across the WAN links. We wanted to avoid connections to the Internet or download from one central server for every remote workstation to update their virus definitions as well.

The following list summarizes the antivirus management system design requirements I established for Company X:

- Install and configure Norton Antivirus 2.15 on Company X's Exchange Server to protect the mailboxes and public folders. Alert us when a virus infects a user's mailbox or public folder.
- Deploy a distributed but centrally managed solution on Windows 2000 Professional Workstations on the remote LANs.
- Load Symantec System Center, Alert Management System, and the antivirus server and client distribution software on Windows 2000 Professional Workstations.
- Designate these Windows 2000 Professional workstations as Local Antivirus Management Stations (LAMS).
- Configure these LAMS workstations to boot up without a monitor, keyboard, or mouse; enable remote control of the LAMS workstation to install Antivirus client software to locally attached laptops and workstations. Setup distribution shares and network print queues for local software installs and printing to local network printers on the LAMS workstations.
- Install and configure PCAnyWhere 10.0 with only the Host piece. Configure PCAnyWhere host access to only allow members of specific Domain Groups. Configure these specific Domain Groups to have administrative rights to the LAMS workstations as well.
- Create Sever Groups for each remote LAN, and designate the respective LAM workstation as the primary parent server of the group.
- Configure each LAMS workstation to manage their local client's policy, distribute virus definitions to the local clients, and report to the Primary server any virus alerts from their managed client install base.
- Configure each LAMS workstation to use the Virus Definition Transport Method (VDTM) to make a connection to the Internet every morning, around 0300ET. The LAMS workstations will download and then distribute the virus definitions to their managed clients, if online, or when the clients contact the parent server.
- Deploy LAMS workstations to remote sites where there are more than 10 workstations on the particular LAN.
- Configure the Antivirus clients to check for updates from their parent server once per day.
- Configure all client real time and scanning options to check all file types.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Configure the client antivirus engine action to repair the file, or delete it if the repair was unsuccessful. This action is the same for macro and non-macro viruses.
- Lock all the configuration settings and password protect the Antivirus Client service. This prevents the users from unloading the Antivirus Service.
- Configure the Alert Management System (AMS2) on each LAMS workstation to send email alerts to administrators and support staff when a virus is found or detected on any managed host.

The WAN and LAN layout

Company X's network is spread out across the continental United States in a mesh configuration, and connected together via a national carrier's frame relay network to the central site datacenter, and the backup datacenter. The backup datacenter is in a different state then the central site data center. All of the major applications, business services, email, IS Staff, and domain functions are located in the central site's data center. The remote site routers are configured with weighted routes to first route to the central site, and if unavailable then route to the backup datacenter. The backup datacenter has a secondary dedicated connection to the central site for routing remote site connections which cannot make a connection to the central site over their primary frame connection.

Norton Antivirus for Exchange Server - Configuration

Company X's Microsoft Exchange 5.5 Server was running on a Windows NT 4.0 Server. Company X had about 1000 user accounts enabled for both internal and external email. Company X had installed Norton Antivirus for Exchange version 2.15 on its Exchange 5.5 server to stop email borne viruses in all user mailboxes and in the public folders. The next step was to ensure that virus definitions were updated frequently. We configured Live Update to check for virus definitions 10 times a month. This was the maximum frequency allowed by the application. We configured the email alerts for any viruses found to be sent to the Exchange System Administrators, the sender of the email, and the recipient of the email.

Upgrade Process – Central Site

After some initial testing on Company X's test network we were ready to proceed. First I set up Company X's Primary server in the central site. I configured Company X's base policy, and spent the next month upgrading all the servers, and central site laptops and workstations from version 4.X/5.X to version 7.51. All the servers had Norton Antivirus 5.02 and Windows NT4.0 SP6a, but many workstations were still on Norton Antivirus 4.X and Windows NT4.0 SP4. We manually installed Norton Antivirus 7.51 CE on a number of the key application servers to ensure there were no conflicts with the existing applications and the installation of Norton Antivirus on the servers. We pushed the install set from the primary server to the remaining central site servers, and to all of the central site

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

laptops and workstations. Those servers, laptops, and workstations which would not upgrade via the push installation method, through Symantec System Center, had to be manually upgraded. The problem with these workstations was they were running Windows NT4.0 SP4 and needed some dll file upgraded. The easiest way to solve this problem was to upgrade the workstations to Company X's current standard of Windows NT4.0 SP6a. This doesn't agree with Symantec's minimum requirements for a Windows NT4.0 Server or Workstation install of Norton Antivirus Client 7.6 CE which is Windows NT4.0 Service Pack 3 or higher.

Symantec released version 7.6 of their Norton Antivirus Corporate Edition suite just as Company X finished upgrading all the central site servers to version 7.51. I spent the next couple of months evaluating, testing, and helping Company X upgrade the all central site servers, workstations, and laptops to version 7.6.

Since Company X does not allow the users to have administrative access to their workstations and Company X does not have a software delivery package, we had to manually install the software. We had the Support Center Technicians manually install Windows NT4.0 SP6a and install Norton Antivirus 7.6 CE from the Windows share I set up on the Primary Server. We were able to push the install to 95% of the servers and 60% of the laptops and workstations.

Upgrade Process – Remote Sites

After I got budget approval to purchase the workstations, the next step was to build the LAMS workstation configuration to support Company X's requirements. Once the LAMS workstation configuration was agreed upon we cloned the image, and replicated the image to the remaining LAMS workstations. We installed two of the LAMS workstations in nearby remote sites to ensure Company X's configuration was correct. We made some minor adjustments to ensure that most of the standard print drivers and all the distribution software were loaded. We configured the BIOS to boot the LAMS workstation when power was restored. After some minor tweaking, we shipped the 30 cloned LAMS workstations out to the remote sites. We provided the site with basic instructions for the remote site contact's to use when installing the workstation in the primary wiring closet. All that was required was a power and network connection for the workstation.

The installation of Norton Antivirus 7.6 CE on the client laptops, servers, and workstations running Norton AV 5.x was seamless for Windows NT4.0 SP6a workstations. Support Center Technicians simply connected to the LAMS workstation with PCAnywhere, opened Symantec System Center (SSC), and pushed the installation set to the local network hosts. The Support Center Technician could run eight installs at one time. Any installations which failed were identified in SSC, and automatically rolled back to Antivirus 4.x/5.x. The next step was to work with the Support Center to ensure that the prerequisites were installed on those identified workstations. Every workstation identified was

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

running Windows NT4.0 SP4 or SP5. This is where the cooperation of the users working with the Support Center Staff came into play.

Upgrade Process - Support Center & End Users

The Support Center staff was tasked with coordinating the installation of Windows NT 4.0 SP6a, as well as deploying Norton Antivirus 7.6 CE throughout the company's extensive network. Company X did not allow users to have administrative rights to their workstations, and Company X did not have a central workstation management software package installed; therefore I employed a couple of inventive techniques to enable the users to install Windows NT 4.0 SP 6a. One of these techniques was to create a domain global group called PCAdmin, and then add the PCAdmin domain global group to the local administrators group on every workstation and laptop. Then, when the need would arise the Support Center staff would add the domain user account to the Domain global group PCAdmin, and have the user logout and log back into the domain. Then the user had local administrative rights to install Windows NT 4.0 SP6a from their Local Antivirus Management Station (LAMS) distribution share. We gave the Support Center Staff PCAnyWhere access to the LAMS workstations. After this was accomplished the Support Center could remotely install Norton Antivirus 7.6 CE on the workstations and laptops from the LAMS workstation. The LAMS workstations had a distribution share for all domain users to access for installing applications, service packs, and hot fixes as well.

The LAMS workstation Antivirus Configuration Policy

- Each remote site is configured with one sever group and one primary parent server (LAMS).
- Each LAMS workstation downloads virus definitions each morning from the Internet.
- The Antivirus clients check for updates from their parent server (LAMS) once per day.
- Client real time and scanning options are set to check all file types.
- The client antivirus engine will try to repair the infected file, or delete it if the repair was unsuccessful.
- The same action is set for macro and non-macro viruses.
- All configurable settings are locked.
- The Antivirus Service is password protected to prevent users from unloading it.
- Alert management on each LAMS workstation is configured to send an email to the administrators, with the subject indicating the location the message came from for each managed host, where the virus came from, what the virus name is, what action was taken by the antivirus engine, and what is the current status.

Symantec System Center – Operation and Maintenance

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Symantec System Center is the central management interface for the Norton Antivirus 7.6 Corporate Edition suite, and ties the policy management, monitoring, reporting, and maintenance functions together. Company X's environment consists of one server group for each remote location, and a parent server under each group. The groups are identified by the site name. Figure 1 indicates each parent server connects to the Internet for virus definition updates via an http request to Symantec's web site and downloads the virus definitions via the FTP protocol. The virus definitions are pushed to the clients if connected to the parent server at the time or when the user boots up and logs into the network. The policy configuration is the same for each group, but virus definition updates and management of the clients is distributed to each group. Therefore if one of the parent servers is offline it doesn't affect the entire system.

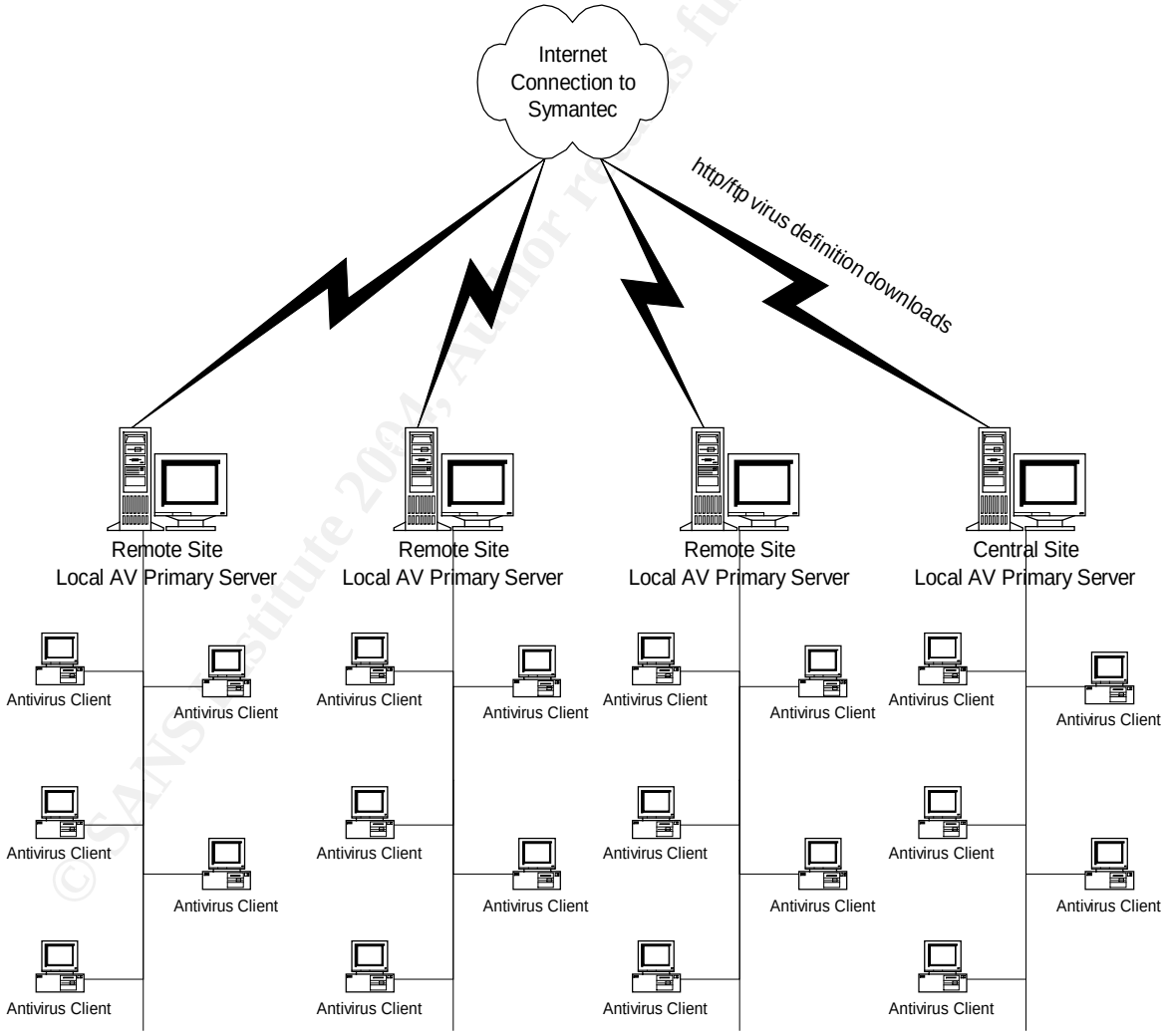

Figure - 1 Symantec Antivirus Architecture

IS Department Responsibilities

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Support Center is the central communications point for all virus activity. Company X's user community has been notified that they need to alert the Support Center if they receive or suspect virus activity on their systems. When the Support Center receives a virus alert they are responsible for ensuring that network administrators are notified in a timely manner. The network administrators are responsible for isolating and eradicating any virus infection, and reporting on their findings to the IS Management Team. The Security Specialist is responsible for investigating and reporting on possible causes of the virus infection and to formulate a plan to mitigate the risk in the future.

Virus Infection – Examples

Example 1 – VBS/Loveletter.C Alias: "Very Funny", "Joke"

Background

After surviving the initial wave of attacks from the VBS.LoveLetter.A in the spring of 2000 Company X felt pretty lucky. Company X hadn't upgraded the email client yet, and Company X didn't have any file association on the Windows NT4.0 workstations or laptops for the vbs file extension. However by the fall of 2000 we started to test Office 2000 and Outlook 2000, which enable the vbs file type to the VBScripting language.

Infection

Company X had two Outlook 2000 users open an email attachment with the subject, Very Funny, and an attachment of VeryFunny.vbs. This was the VBS/Loveletter.C variant. These two users infected several hundred email mailboxes, and contaminated several network shares.

Eradication

Company X had these two users disconnected from the network within 10 minutes, but before we could get to their workstations significant damage had been done. Several thousand jpg files stored on network shares throughout the company were infected. We had to take the Exchange server off the Internet for a day to clean up the mess. This is when we discovered a new tool Microsoft had released to support cleaning up user mailboxes. The **Xmerge.exe** utility allowed us to clean infected mailboxes before the users could open them. **Xmerge.exe** allowed us to run a scan on every Exchange user mailbox and filter out emails based on specific criteria, such as attachment name, attachment type, subject, from, or to. After the Exchange server was cleaned we moved onto cleaning up the mess on the file servers. We searched the network for jpg.vbs files and restored all these files from tape.

Mitigation

Next Company X needed to reevaluate what changes we should implement going forward. Company X's current antivirus standard for the servers,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

workstations, and laptops was Norton Antivirus 4.x/5.x and it did not have email protection capabilities. We developed the following strategy:

- Review Company X's Antivirus Response Plan, and update as needed.
- Send an email to the user community, emphasizing the importance of not trusting email attachments; and to scrutinize any unexpected email attachment received. "Train employees not to open attachments unless they are expecting them."[2]
- Implement a Norton Antivirus for Exchange Attachment Blocking Policy to include *.com, *.exe, and .vbs files.
- Test and determine why Norton Antivirus 5.02 did not detect the virus and stop it.
- Test Norton Antivirus 7.5 Corporate Edition, which has Exchange email protection built in.
- Begin a rollout plan for upgrading the environment to Norton Antivirus 7.5 Corporate Edition.

Example 2 – W32/Nimda-A Alias: W32.Nimda.A@mm

Example 2
The W32/Nimda-A
Background

During the summer of 2001 Company X installed and configured their first production web server. Company X had a full development team running web services on their workstations and laptops; and testing various code builds prior to installing on the production environment. There were several warnings on the Internet about the W32/Nimda-A worm causing havoc. Company X expeditiously updated all of the servers and workstations with new virus definitions as soon as they were released preparing for the worst.

Infection

The afternoon of September 20, 2001 Company X got the first taste of the W32/Nimda-A worm. The users were asked to run an antivirus scan on their workstations. Several users called the Support Center after running their virus scans and reported that Norton Antivirus 5.02 was popping up message alerts on their workstations or laptops. Something wasn't quite right. The popup messages reported infected files were quarantined on their workstations and laptops as a result of the W32.Nimda.A@mm worm. Then we received reports from the developers indicating their web servers were not working.

Eradication

We disconnected the developers from the network and upgraded their Antivirus engine from Norton Antivirus 5.02 to Norton Antivirus 7.51 CE from an installation CD. Next we loaded a new corporate standard build of Internet Explorer, and updated the web services with the latest security patches. Then we ran the Nimda repair tool to make sure we did not miss anything.

[2] http://www.sarc.com/avcenter/venc/data/w32.mimail.d@mm.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Mitigation

Next Company X needed to reevaluate what changes we should implement going forward. It is imperative the users scan their local hard drives going forward until Company X can upgrade all of them to NAV 7.51 CE. We developed the following strategy:

- Expedite the Antivirus upgrade project, since the Norton Antivirus 5.02 auto protect function failed to catch the infection attempts; even though the virus signatures were updated with the W32.Nimda.A@mm signature.
- Review Company X's Antivirus Response Plan, and update as needed.
- Remind the users it is imperative to scan their local hard drives going forward until Company X can upgrade all of them to NAV 7.51 CE.
- Send an email to the user community to use the Internet for business purposes and to review the Internet Policy if they have any questions.
- Begin the rollout of Norton Antivirus 7.51 Corporate Edition.

Norton Antivirus for Exchange Policy Changes

Company X's first significant policy change was to implement an attachment blocking policy as recommended by Symantec's Antivirus Research Center. Company X knew there was a gap in time between an antivirus signature update for a rapidly spreading virus in the wild and when a virus may hit Company X's network.

Plus, the Norton Antivirus for Exchange application only allowed 10 Live Updates a month. Company X needed a stop gap measure to ensure that we did not receive any new viruses before the antivirus signature updates were installed. A quick visit to the Symantec Antivirus Research Center web site and a lookup of any virus today will provide a list of which file attachment types to block, "Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files."[3]

Norton Antivirus for Exchange provides a means to block attachment types via the registry. The registry key "HKLM\SOFTWARE\Symantec\NAVMSE\2.1\BlockingPolicy\Attachment" Allowed us to add a number of attachment types to block. We decided to initially block .exe, .com, and .vbs files. We needed to make sure Company X did not affect email attachments the business was using. Shortly after implementing the new attachment blocking policy the quarantine log displayed a large number of jokes and programs the users were receiving from Internet email addresses and internal Exchange users. The amount of executables floating around via email was amazing. Just imagine how many potential Trojan horses the email users could have received via attached executable joke files.

[3] http://www.sarc.com/avcenter/venc/data/w32.marque.worm.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Once the initial Norton Antivirus for Exchange attachment blocking policies were implemented all the Loveletter.vbs variants and other copycat vbs viruses, which were exploding all over the Internet at the time, were received by the Exchange server and dropped into the quarantine folder for review. As new viruses exploited other attachment types we updated the attachment blocking policy to prevent new virus infections. The toughest attachment type to block was the .bat file type due to the internal email use of batch files for updating various things for Company X's users. However, we did implement the .bat file type, to the blocking policy prior to the outbreak of a number of worms utilizing .bat file extension; including the infamous W32.Sircam.Worm@mm mass mailing worm. Company X's updated blocking policy includes .bat, .cmd, .com, .exe, .mp3, .msi, .pif, .reg, .scr, and .vbe files. Company X blocked most known virus file attachments. Company X had several months where the quarantine folder had well over a 1000 blocked attachments per month. We monitored the Symantec Antivirus Research Center web site daily to keep abreast of any new file attachment types to consider blocking.

Antivirus Communication

Today Company X has Norton AV 7.6 CE installed on all the servers, workstations, and laptops. The virus alerts we configured have worked very well to identify whose workstation or laptop was attacked by malware. The virus alerts along have increased Company X's ability to respond to virus outbreaks, because, to this day, users tend to not call the Support Center to report virus alerts they receive on their own workstation or laptop. Today Company X administrators are alerted via email as soon as the infection happens, speeding up recovery time.

Virus eradication - Examples

Example 1

Relying on Company X's users to not open email attachments is probably one of the biggest difficulties in protecting the internal network from the outside world. We have seen several VBScript viruses attempt to infect Company X's email system, such as the AnnaKournikova.jpg.vbs worm. Company X's attachment blocking policy has been working to perfection, and it is tested regularly by live viruses and unauthorized file attachments almost every day.

Example 2

Company X had just implemented a blocking policy for the program information file extension .pif when the W32.Badtran made headlines around the Internet, and a posting on Symantec's Antivirus Research Center web site.[4] We were able avoid any worms using the pif file extension.

Example 3

[4] http://securityresponse.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Several months later Company X added the screen saver file extension .scr to the attachment blocking policy on the Exchange server; the following week the W32/Goner Worm, made headlines across the Internet. The CERT® Coordination Center posted Incident Note IN-2001-15, explaining the significance of this worm.[5] Again, we were able avoid any worms using the scr file extension.

Example 4
Company X's Internet mail enabled mailboxes, on the Exchange server's public folder store were receiving a number of infected attachments, but Norton Antivirus for Exchange was not detecting the infected emails. Norton Antivirus 7.6 CE, on the workstations and laptops, did detect and quarantine the viruses when the user opened the emails with their (Microsoft Outlook 97/98/2000) client.

Security environment changes - Defense in depth

As I pointed out earlier, Company X had a problem with the spread of viruses through web email. The network support team updated the email policy and required all users to sign the email policy annually. The network support team implemented email attachment blocking policies to combat email worms. The network support staff changed the company's email practices to send email links and not attachments for internal email.

We installed and implemented a couple of different network devices to control which protocols and applications communicate from the internal network to Internet hosts.

After significant research time Company X implemented a new firewall and web filtering system. These two devices significantly reduced the risk of web email borne viruses.

[5] http://www.cert.org/incident_notes/IN-2001-15.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Antivirus Software Technology - Changes

Microsoft has made significant improvements to their email client software. Microsoft Outlook 2002 comes standard with a blocking policy set to block all executables attached to emails.[6]

The good news is Symantec, along with their competitors, has been pressured to upgrade the capabilities of their Antivirus software to detect several new threats, as well as protect the email client software.

Conclusion

Antivirus software will continue to evolve into a Security product capable of detecting all of these threats, tracking intrusion attempts, and providing basic firewall, and application baseline protection, but not today. "Protecting your business from a virus outbreak is harder than ever. Just ask Microsoft. Last January, Microsoft was hit with the SQL Slammer virus, which infiltrated the company's own Web servers. Microsoft had known about the vulnerability in its SQL Server database but failed to patch all its systems…"[7] The viruses and worms of today are evolving into blended threats with multiple capabilities tomorrow. The Internet community as a whole needs to improve their protection systems from the blended threats of tomorrow to protect us all.

The security staff will continue to improve the security protection systems at Company X, and protect the Internet community from any malware infections on Company X's systems.

© SANS Institute 2004, Author retains full rights.

[6] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/office/officexp/reskit/html/outg01.asp

[7] Corporate Antivirus Software, By Jay Munro April 22, 2003")
<http://www.pcmag.com/article2/0,4149,992730,00.asp

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix A – Malware Threats

The list below is from Symantec's web site and defines these threats.[8]

Types of Threats:

- *Adware*
  Programs that secretly gather personal information through the Internet and relay it back to another computer, generally for advertising purposes. This is often accomplished by tracking information related to Internet browser usage or habits. Adware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. A user may unknowingly trigger adware by accepting an End User License Agreement from a software program linked to the adware.

- *Dialers*
  Programs that use a system, without your permission or knowledge, to dial out through the Internet to a 900 number or FTP site, typically to accrue charges.

- *Hack Tools*
  Tools used by a hacker to gain unauthorized access to your computer. One example of a hack tool is a keystroke logger -- a program that tracks and records individual keystrokes and can send this information back to the hacker.

- *Hoax*
  Usually an email that gets mailed in chain letter fashion describing some devastating, highly unlikely type of virus. Hoaxes are detectable as having no file attachment, no reference to a third party who can validate the claim, and by the general tone of the message.

- *Joke Programs*
  Programs that change or interrupt the normal behavior of your computer, creating a general distraction or nuisance. Harmless programs that cause various benign activities to display on your computer (for example, an unexpected screen saver).

- *Remote Access*
  Programs that allow another computer to gain information or to attack or alter your computer, usually over the Internet. Remote access programs detected in virus scans may be recognizable commercial software, which are brought to the user's attention during the scan.

[8] http://securityresponse.symantec.com/avcenter/refa.html#security

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- *Spyware*
  Stand-alone programs that can secretly monitor system activity. These may detect passwords or other confidential information and transmit them to another computer. Spyware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. A user may unknowingly trigger spyware by accepting an End User License Agreement from a software program linked to the spyware.

- *Trojan Horse*
  A program that neither replicates nor copies itself, but causes damage or compromises the security of the computer. Typically, an individual emails a Trojan Horse to you-it does not email itself-and it may arrive in the form of a joke program or software of some sort.

- *Virus*
  A program or code that replicates; that is, infects another program, boot sector, partition sector, or document that supports macros, by inserting itself or attaching itself to that medium. Most viruses only replicate, though, many do a large amount of damage as well.

- *Worm*
  A program that makes copies of itself; for example, from one disk drive to another, or by copying itself using email or another transport mechanism. The worm may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software of some sort.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

LIST OF REFERENCES

Book References:

"SANS Security Essentials with CISSP CBK" version 2.1 volume 2, page 1056

Internet Sources (URLs):

Symantec Corporation Web Site:
http://www.symantec.com

Norton Antivirus Corporate Edition Product Page
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155&EID=0

Symantec Enterprise Security Products Web Page
http://enterprisesecurity.symantec.com/products

Symantec Antivirus Research Center
http://www.sarc.com

Symantec Antivirus Research Center – Virus Name Write Up
http://www.sarc.com/avcenter/venc/data/w32.mimail.d@mm.html

Symantec Antivirus Research Center W32.BadTrans@mm.html – Write Up
http://securityresponse.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.html

The CERT® Coordination Center Incident Note IN-2001-15 W32/Goner Worm
http://www.cert.org/incident_notes/IN-2001-15.html

Customizing the Outlook Security Features Administrative Package
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/office/officexp/reskit/html/outg01.asp>

Munro, Jay. "Corporate Antivirus Software." April 22, 2003.
http://www.pcmag.com/article2/0,4149,992730,00.asp

Symantec Security Response – Glossary
http://securityresponse.symantec.com/avcenter/refa.html#security

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: July 22nd, 2017

Upcoming Training

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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor