Global Information Assurance Certification Paper

Case Study: A Prong Approach
GSEC Practical

Michael Forney
GIAC Security Essentials Course GSEC
June 21, 2004

Abstract

With Spam, Mallware, and viruses propagating the internet at an all-time high, this case study details the process implemented in my organization to lessen the impact of these malicious attacks. I will take you on a journey which includes developing and Internet and E-mail Usage Policy, implement enterprise wide anti-virus protection with centralized management, and analyze internet traffic patterns. This will also include replacing an outdated firewall, upgrading the messaging system, and migrating to a network operating system (NOS) designed for computing in the twenty-first century. Obviously, all this would be useless if proper training is not provided.

Before- Understand Your Past

This journey takes place at the company I have been employed by for a considerable amount pf time. I remember a conversation I had with the MIS director from my younger days at the company. The internet was young web browsing, and we were just getting on board. I mentioned something bout security and preventing hackers from getting into our network. His response was "We have never been hacked or lost any data we couldn't recreate." Over the years, I came to realize this was the attitude of the entire management team. I remember getting responses like "We haven't been hacked; we'll cross that bridge when we get to it," or "we're a small company and no one is interested in hacking our network." But my all time favorite was "We picked this small town in the middle of nowhere so that we could stay away from that type of activity." These attitudes were evident in the lack of an internet usage policy. Microsoft Proxy Server was used as a firewall. The log files were only to be looked at if management suspected abuse. Unbeknownst to the organization, the mail server was configured as an open relay server. MacAfee Antivirus was installed on most workstations, but updates were left to the end-user. NT Servers were patched on a whim and workstations were never patched.

During: The Journey Begins

This journey begins sometime in the year 2000 when the company moved to Microsoft NT and Exchange 5.5. The company up to this point was on all Novell Shop running a messaging package called Noteworks for Netware. Noteworks was bought by a company that was not going to provide support for the package any long, the company hired an external consultant to recommend and build an infrastructure, which would allow internal and external communication. The infrastructure was a Windows NT 4.0 Domain with Exchange 5.5. The company then on the recommendation of the consultant hired another consulting firm to implement a firewall. The firewall chosen was an Arent Raptor software firewall. The implementation went well, the company put up a web server, had corporate wide internet access, internet email, we put up an intranet site, and Outlook Web Access Server for our store managers. There was only one problem, the company, despite

providing training for Windows and Exchange; they would not provide the training for the Raptor Firewall. At that time, there were no books on the Raptor Firewall, nor were there many user forums covering the system. As the network administrator, I stated to the IT Director that no one on our staff understood how the Raptor System worked and explained that you don't just install a firewall and not manage it. Unfortunately, the response was more of the same- "If we have a problem we'll call the consultant firm back for assistance. Over time, I did eventually learn the Raptor System, but it came at the expense of reactionary firefighting.

Our first major problem came when I got that dreaded phone call, "I can't send email to one of our vendors!" We had been experiencing similar problems for about two weeks, but this message came from the president of the company. After doing a considerable amount of research, I was directed open relay database ordb.org. Sure enough we were listed on every major email blacklist as an open relay webopedia.com on a SMTP email server that allows third party to relay email messages. Open relays make it possible for mobile users to connect to corporate networks by going first through a local ISP which then forwards the messages to their home ISP, which then forwards the message to the final destination. Open relays are commonly used by spammers looking to hide their source of the large amounts of email they send. By the time we got that mess cleaned up and email flowing to the world again, the Code Red Virus hit.

Definition
Virus- a program or piece of code that is loaded into a computer without your knowledge and runs against your wishes and commands; may also replace themselves.

Worm- a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

Although our servers managed to dodge the wrath of the Code, several of the workstations were hit hard by the Worm. Because we underestimated the damaged caused by Code Red, Nimda all but crippled out internet infrastructure. We had to shut down our mail server for two days and rebuild two web servers. We spent weeks cleaning up workstations and servers. The clean-up effort was more because we had over100 computers with unprotected dial-up access to the internet access our mail server from all over the country. For the next year or so, I spent a considerable amount of time manually doing patch management and virus updates. All the while our server farm grew from five Windows NT Servers to sixteen. Throw in the five Netware Servers and d you eat, sleep, and breathe patch management. By the time the Sobig virus came out we were hit by every major virus prior to its release. Sobig was no exception, spreading so fast that at least seventy-five percent of our systems were infected by the time we took out mail server off-line. One side affected of so many comprised systems was SPAM.

The amount of SPAM flowing through our mail server was so bad we had users getting over 100 messages per day. We were taken in so much SPAM; I think we were SPAM ourselves.

New Management: New Opportunities

The year was 2003 also brought about new management in the IT infrastructure. Under the old IT management there was very little interest in security. As the network administrator I felt it was my responsibility to use what was at my disposal to keep our network as clean as possible. When management refused to purchase anti-spam systems, I fought back to block as much as I could by taking a daily sample spam and manually sorting them looking for key words, then entering those key words into Exchange 5.5 Keyword Filtering System. Well, anyone that has ever tried fighting SPAM knows that (1) key word filtering will never stop spam and (2) it is very time consuming. With the old management anti-virus updates were a manual process. The techs would be assigned a department, then that tech would manually update the anti-virus software by going to each machine in that department.

The second half of 2003 brought about new IT management. When news of a new IT director hired, I was determined not to let this management allow outside consultants to decide the security of my network and leave me with a bag of squashed apples to clean up. Enough was enough and I was not to be denied. I by the time the new IT director was hired; I would have a complete layout of what I thought this company's network should look like form a security perspective. The plan would be to include centralized anti-virus distribution and management replacing the firewall, upgrading the mail server, and the Domain Structure.

The first step was to document what was happening on the network. For this I used programs (tools), Network Associates ePolicy Orchestra, Webtrends, and a program named Promodag.

ePolicy Orchestrator is Network Associate's anti-virus distribution and management engine. With ePolicy Orchestrator, I was able to automate the distribution of the McAfee client agent to 185 computers throughout the building. Once the agent was installed I could then generate reports detailing our anti-virus coverage and the extent of the virus infection.

The next step was to put together a baseline for the amount of SPAM coming into and exciting our mail server for these reports I purchased a program named Promodag. Promodag allowed us to measure the usage of our mail server and analyze traffic patterns.

With Promodag I generated reports detailing incoming mail traffic to determine which servers were receiving excessive amounts of email. Reports were generated for outgoing mail to determine if some of our internal systems were flooding our mail server. Reports were also created detailing which mailboxes actually contained viruses in attachments.

The final step to document that was happening on the network was to determine how the internet was being used by our users. In our company this was a very sensitive subject because there was no Internet Policy, users could do what they saw fit while on the internet. I approached the CFO who was also acting IT director at the time and indicated that some of our problem with SPAM and virus is directly related what our users are doing on the internet. And requested permission to look through the logs and run some reports. Permission was granted only after I threw out some statistics on how the Internet use affected worker productivity.

They way some people see everything as black and white; well, accountants see everything as black and red. If you tell an accountant they are losing money because of lack of productivity, they start to quiver and get anxious. They want to know what the extent of the problem is and how to stop the hemorrhaging.

We had a license for one of the first editions of Webtrends Reporting Software. I looked it and created some reports from our proxy server logs. Webtrends led us in the right direction, but it was too outdated to interpret all the information from the log files.

We purchased a product called Sawmill, which enabled us to generate reports on how much time users spent on the Internet, who spent the most time browsing, and which sites were being hit the most. It also allowed us to see what users downloaded and who was using adware.

The internet usage reports were unbelievable. There were people spending as much as three and a half hours a day on the internet, browsing topics from sports, gambling, and stocks to growing and selling illegal drugs, and pornography.

Mindful that the initial reports were probably skewed by the amount of spam we were receiving, I set filters to track usage by the length of time spent on each site. The results were the same people were spending too much time on internet for non-work related and sometimes unethical and/or illegal purposes.

When presented the usage reports the CFO was furious and obviously wanted action taken immediately. I informed the CFO/IT Director there was nothing we could do with the reports because the company did not have an Internet Usage Policy. I further explained the need of a policy informing users what is acceptable and what is not in terms of the Internet usage from the company. From that discussion, we set out to develop an Internet usage policy. We were now on our way to securing our network.

Using templates and documentation from the web sites listed below, we drafted an acceptable internet and Email Usage Policy.

1. http://www.sns.org/resources/policiesthe
2. security handbook at http://www.ietf.org

The final document was a collaboration effort, which included members from the IT Department, Human Resources, the company's legal team, and the management staff.

Armed with an acceptable Usage Policy, documentation on usage patterns, email traffic, anti-virus coverage, and a history of consulting mishaps, I was set to approach the new IT management with the plans to clean up the mess and solidify our network.

The plan was to upgrade and take full advantage of Network Associates Total Virus Defense and replace the Raptor (now Symantec Enterprise Firewall/VPN) with a Cisco PIX. The plan was aggressive, but the new management approved it with a few additions. We would use Internet Filtering to supplement the usage policy, use four firewalls to support wide area network instead of one PIX firewall, and take the GSEC course and exam. I got more than I asked for, but in this case more was definitely better.

ePolicy Orchestrator

The first phase was to strengthen our anti-virus protection. For this I again employed the services of Network Associated ePolicy Orchestra. This time upgrading to version 3.5. We had trouble getting the previous version of 3.0 working on our environment. With ePolicy Orchestra up and running, I used discovery feature to find every computer on the network. The ePolicy Orchestrator Server was configured to pull updates from Network Associates update server everyday and a special outbreak rule was created to pull updated every four hours during an outbreak. The client agent was configured to receive updates first from the ePolicy Server, and then pull from Network Associate's FTP Server. To reduce network traffic, servers received updates once a day, while workstations received updates twice a week. Then I grouped every system by the department in which it was associated with. The configuration would be useful for distribution of updates, monitoring outbreaks and generating reports. When all the computers were grouped

by department, rules were created to distribute the new client agent all the workstations and servers. The servers received their updates immediately and were scheduled to receive their updates in the evening. Once the agent was distributed to all systems I generated a protection coverage summary report. Coverage was dismal, many more machines were using outdated software, scan engines that had not been updated software in as many as two years, virus definition files were not being updated and some systems did not even have anti-virus software at all. The worse case was the backup server, which had no virus protection.
Next, rules were created to distribute the latest software, engine, and definition files to all servers and work stations. Now that all systems were protected, it was time to eradicate some bugs. ePolicy Orchestrator has a broad list of reports managing and monitoring virus activity. Among the more popular reports, is the number of infected computers and virus infected computers. The base configuration for all computers was

1. Scan all local drives
2. Scan once a day (12:00pm)
3. Scan all files (including mime and compressed)
4. Upon deletion clean file, delete if clean failed

Servers are scanned twice at 4:30pm before nightly backups and 5:00am after the previous night's poll. The amount of viruses propagating our network was incredible. There were some computers with over 150 instances of Netsky in a week. We were able to clean the network by killing the viruses before they spread, but now we needed to stop them at the door.

Cisco PIX Secure Firewall

I chose the Cisco PIX Secure Firewall because of comfort level. Having installed several smaller units before including the unit in my home network, I had a good understanding of how the IOS worked. So I contacted Cisco's Pre-sales division. The plan was to install four units, one for the corporate office, and three for the wide area network.

A brief understanding

Our WAN will connect over 100 of nationwide store locations to the host site (corporate office) via xDSL into a private ATM network. Prior to this project are if a store on the WAN wanted to go to ups.com that store would come through the WAN to LAN through the proxy server that through the firewall to the Internet and back. We needed to reduce the latency created by an inefficient network design.

Our goal was to install three Cisco PIX 506 firewalls in our WAN Providers egress points. These units would be geographically placed to service the Internet needs of our WAN sites. One for the east coast a, one for the Midwest, and one for the west coast. This design would reduce the latency caused by traveling from the west coast to the east and back for a web page. This design also had another important function. We needed to separate the store Internet traffic from the corporate Internet traffic. Our plan was to shut off Internet access from the remote sites, and then turn on a pre-selected list of websites as determined by business need.

Selecting a firewall for the remotes sites was a gimme. We needed a unit that could handle very small amounts of traffic for a maximum of ninety simultaneous users. The unit would be implemented solely for the purposes of keeping people out. This meant no VPN users, no web hasting. All management would be done over the private network. Because of these limited needs we chose the Cisco PIX Firewall 506.

The replacement firewall was a different story. This unit had to handle the traffic of over 200 internal users; the unit needed multiple interfaces (no less than three). The system also needed traffic for medium site website, an extra-net site, VPN, and a host of other services. We need something bigger than PIX 506. Although the Cisco Pre-sales contract informed is that 515 would meet our needs, the management team wanted to go with the PIX 535. We comprised and selected the PIX 526ur (see chart).

PIX Firewall	**515-UR**	**525-UR**	**535-UR**
Software	6.3(3)	6.3(3)	6.3(3)
Licensed Users	Unlimited	Unlimited	Unlimited
VPN Users	Unlimited	Unlimited	Unlimited
Processor (MHz)	200	600	1024
Base RAM	64	256	1024
Flash (Mb)	16	16	16
PCI Slots	2	3	9
Maximum Ports	8	8	8
Fail over	Yes	Yes	Yes
Firewall Throughput	145	320	1,700
3DES Throughput (Mbps)	10	70	95

Since this was a replacement firewall all of surrounding components were already in place. This meant that the unit had to be built and configured in the lab environment because once we made the switch the entire internet infrastructure would be down if something went wrong.

With the firewalls in place it was time to implement web filtering and reporting. There are only two products certified by Cisco to interoperate with the PIX: N2H2 and Websense. Unfamiliar with these products, I evaluated both of them. The criteria used for evaluating the software were as listed:

1. Is the database comprehensive?
2. Is it accurate?
3. Are the database updates provided automatically?
4. Ca we add custom categories
5. How easy is the installation
6. Is there a web interface for management?
7. Is the solution scalable?
8. Can I centrally manage multiple sites?
9. Are the reports customizable?
10. Does it actually block what it is supposed to
11. Is the price appropriate for your needs?
12. How flexible is the licensing
13. What if you need small increments of users?
14. Is it capable of alerting administrators in the event of errors?
15. Can you administer everything from one location?

N2H2's Sentian product was chosen because of the products ease of installation and use, the accuracy of the database, its pricing model, and successful blocking accuracy.

Content filtering for the remote firewalls were straightforward because we turned off the Internet.

Content filtering for the remote firewalls are pretty straightforward because we turned off the Internet with the exception of a few business related sites. For this reason I will focus on the corporate firewall.

The first step was to build the computer that would do the filtering. Our filtering server was a Win2K3 Server with

1. Dell Optiplex GX270
2. 3.2 GHz Pentium
3. 1 GB of Ram
4. 120 GB HDD
5. IIS 6.0
6. SQL Server 2000
7. .Net Framework 1.1

Once the server was configured and the filtering software installed I configured with basic business filtering as our Internet usage policy details. The basic business filtering option in Sentain is more restrictive that out Internet policy but again that's a good thing.

The results

When the Internet was introduced to our company, I remember the MIS Director saying the Internet and web browsing was just another computer fad. That statement may have led to the overall view of "If it isn't broken, don't try to fix it" policy when dealing with the issues of Internet security. Using the basic principles of the Security Essentials Course out company is better prepared to handle the volatile and intrusive nature of the Internet. We have an Internet and Email Usage Policy that will protect the network from our users and increase user productivity. As a result of Network Associate ePolicy Orchestrator and Virus scan, we have not experienced an infected system. With the Cisco PIX firewalls, our users can work with the confidence that their data is safe.

References

ALA American Library Association
http://www.ala.org/ala/pla/plapubs/technotes/internetfiltering.htm

N2H2
http://n2h2.com/products/sentian_home.php

SANS
http://www.sans.org/resources/policies/#template

DynaComm
http://www.dciseries.com/documentation/dcifilter/choosing_internet.pdf

Websense
http://www.websense.com

Tek-tips User Forum
http://www.tek-tips.com

Cisco Discussion Forums
http://forum.cisco.com/eforum/servlet/NetProf?page=main

Hardening Network Infrastructure
Wesley J. Noonan, Roberta Bragg

Cisco PIX Firewalls
Robert Deal

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS 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
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
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
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
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