Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Case Study: Providing malware outbreak protection for controlled and uncontrolled zones within a university

Many environments find it difficult at best to ensure the security posture of the devices under their direct control. Universities and like organizations have to tackle this problem without the ability to administratively control many of the computers attached to the network. This case study will examine a method of providing protection in an automated fashion utilizing security technologies and products from Cisco Systems. We will be following a systematic framework for determining cost/benefit justification of the pr...

Copyright SANS Institute
Author Retains Full Rights

AD

Case Study: Providing malware outbreak protection for controlled and uncontrolled zones within a university

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 2 - Case Study in
Information Security

Submitted by: Chris Jackson
Location: On-Line
Date Submitted: 11 August 2004

Paper Abstract: Many environments find it difficult at best to ensure the security posture of the devices under their direct control. Universities and like organizations have to tackle this problem without the ability to administratively control many of the computers attached to the network. This case study will examine a method of providing protection in an automated fashion utilizing security technologies and products from Cisco Systems. We will be following a systematic framework for determining cost/benefit justification of the proposed solution to ensure it meets the security and budget needs.

© SANS Institute 2004, Author retains full rights.

Table of Contents

Abstract/Summary 1
Case Study Background 1
Security Environment and Network Background 1
The Problem Description 3
The Issues 3
Threats identified 4
Determining the solution 4
The ASIS International Guidelines 4
Step 1 Understand the organization, the people, and assets at risk. 5
Step 2 Specify loss risk events/vulnerabilities. 5
Step 3 Establish the probability of loss risk and the frequency of events. 5
Step 4 Determine the impact of the events. 6
Step 5 Develop options to mitigate risks. 6
Step 6 Study the feasibility of implementation of options. 8
Step 7 Perform a cost/benefit analysis. 9
The Solution in Action 11
Conclusion 12
References 13

© SANS Institute 2004, Author retains full rights.

Abstract/Summary

The Webopedia defines malware as:

Malware:(mal´wãr) (n.) Short for malicious software, software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.[1]

This generic term is one of the most difficult problems facing the security community today. The number of discovered vulnerabilities and those individuals willing to write code to exploit them is rapidly increasing. CERT statistics show that the number of reported incidents is increasing year over year. In 2003 there were over 137,529 incidents reported. These numbers are hard to quantify due to the fact that these were only the reported incidents and may represent an attack on a small number of hosts or thousands. [2] The fact of the mater is, vulnerabilities as well as day zero attacks are a major concern for all IT organizations.

Universities are at an even larger disadvantage than most organizations in this battle. They typically have limited budgets and smaller support staff to tackle security and day to day administration. Many times the student population and the subnets they are connected to are like the wild west in that anything goes and everyone is the sheriff (administrator of their individual PC's). This lack of control from a budgetary and manpower stand point has many university administrators looking to technology to help with this problem. In this paper we will explore a case study of one universities quest to minimize cost, decrease incident exposure levels, and the solutions developed through the process.

Case Study Background

The university that we will be discussing is a small private university of about 3000 students that I had the privilege of working with as a security consultant. My role was to help them to develop a plan to minimize the impact of malware and allow them to automate as many of the security functions as possible so that they could not only do their "day job", but also see their families once in a while.

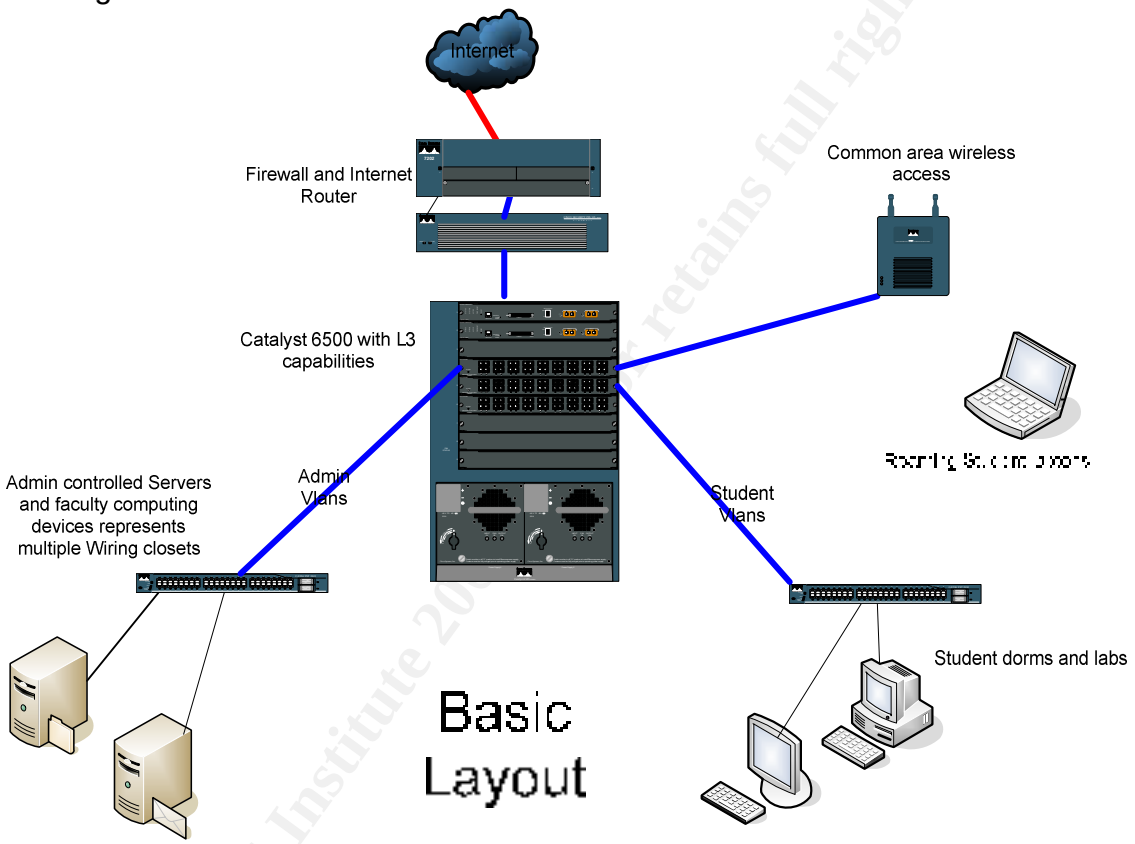
Security Environment and Network Background

Given their budget and staff size the university IT department had done a pretty good job of keeping the key servers and critical systems properly patched. They also actively preformed Nmap[3] and Nessus[4] scans against the core systems to

[1] Webopedia URL:http://www.webopedia.com/TERM/M/malware.html
[2] CERT/CC Statistics 1998-2004 URL:http://www.cert.org/stats/cert_stats.html
[3] Nmap URL:http://www.insecure.org/nmap/
[4] Nessus URL:http://www.nessus.org/

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

test for known vulnerabilities on a monthly basis. Many departments had their own servers and the intranet was utilized for school and class info. The intranet could be reached from the internal network only. These systems we maintained by IT but not completely controlled by IT. IT had standardized on Mcafee Virus Scan Enterprise[5] and configured it to automatically update on a daily basis (midnight). The antivirus clients were deployed on all windows desktops as well as lab pc's. Email was not centrally scanned, as this duty was relegated to the desktop AV client. Desktop patching was accomplished "as needed" with little emphasis placed on staying current. There was also the lack of any automated patching mechanism.



The network was designed with speed and scalability in mind from the ground up. The university had purchased a Cisco Catalyst 6509 and outfitted it with redundant supervisor modules and layer 3 routing engines. The 6500 was in the core of the network and all wiring closet switches connected to it via gigabit Ethernet. Access to the network was accomplished from the wiring closets with a mixture of Catalyst 2900 and 3500 series switches (all layer 2). This switches where configured to trunk their vlans back to the core of the network where the routing function in the 6500 was used to provide a layer 3 boundary. The vlan structure was planned from the beginning with the ability to segment University faculty and administration staff from student vlans. They had a total of 40 vlans serving the school.

[5] Mcafee URL :http://www.mcafee.com/us/

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The core 6500 was connected to a Cisco Pix 525 firewall which then connected to the universities Internet access router, which was a Cisco 7200 with a 45mb internet connection. The University had also started to deploy wireless in common areas (Library, Student Center, Ect), and was providing open authentication (no wep). A seprate group was working on a better authentication and encryption mechanism for the wireless network, so that piece was not part of the scope of this project. No IDS was deployed and visibility into the security posture of the network was near zero. The first IT heard of a problem was through an outage, spike in bandwidth use, or the phone ringing off the hook.

The Problem Description

The Issues

IT had done an admirable job with what they had in place already, but at the time that I was called in they had just experienced the effects of MSBlaster[6] during registration and the first week of school. The outbreak was so bad that their only recourse was to disconnect their internet feed and perform registration via paper and pen. Classes were late or canceled and IT was forced to recruit students in addition to a local IT staff augmentation company to be part of the “sneaker net” they used to run from machine to machine with patching and cleaning software. Needless to say they were motivated to apply countermeasures to prevent the hours of patching and cleaning they were forced to endure and the cost of cleanup.

The other issue they realized is that the main reason that MSBlaster was able to take out the network so effectively, is that they did not have a very good desktop protection strategy. Mandating AV technology only solved the problem for viruses that where know and didn’t help at all with the outbreak of a day zero virus or worm.

In an article posted on TechRepublic John Verry, a consultant for the security firm of CQUR IT, stated in regards to the speed in which SQL Slammer propagated that "antivirus software by its very nature (signature-based detection) is a reactionary technology. Accordingly, any worm with the ability to replicate with the speed and efficiency of an MS/SQL will render antivirus ineffective to block the initial outbreak."[7] This concept of a proactive vs. reactive solution was top of mind to this universities decision maker. A technology that was more immune to the speed at which viruses and worms propagated was required. It was becoming painfully clear that AV technology alone was not enough. E-securityplanet.com provided the average response times of 23 major anti-virus vendors to code and package a new virus definition file after a new virus/worm

[6] SANS Internet Storm Center MSBlaster URL:http://isc.sans.org/diary.php?date=2003-08-11
[7] Bowers, Tony **Lock IT Down: Antivirus software alone is not enough protection** URL:http://techrepublic.com.com/5100-6313-5140210.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

was found in the wild. The average ranges from 6 Hours 51min to almost 30 hours![8] With the pace of newer high-speed worms like sapphire, reactionary technology (signature based) simply can not keep up. The technical report "The Spread of the Sapphire/Slammer Worm" details the speed on this worm: "The Sapphire Worm was the fastest computer worm in history. As it began spreading throughout the Internet, it doubled in size every 8.5 seconds. It infected more than 90 percent of vulnerable hosts within 10 minutes."[9] So ultimately it doesn't matter how large the Anti-virus companies staff Is, these viruses and worms have the ability to beat them to the punch.

The other big problem the university had was the fact that they were not really able to control what students did on their own PC's. The students were also running a multitude of operating systems, from Mac's to Linux. The lack of control and patching issues made it much more difficult to fight these outbreaks. If one vlan had an infected PC the rest of the devices connected would more than likely be infected by the time IT knew about it. IT was accustomed to creating router access control list when a new threat reached the press, but usually by then it was too late.

Threats identified

Ultimately the threats that we felt needed to be addressed immediately as part of the proposed solution were the following:

1. Better control of desktop policy (Faculty and Admin) and zero day worm/virus protection
2. Visibility into the security posture of the network (are we under attack?)
3. Ability to protect the student segments from themselves as well as protect the administration side of the network (faculty and support staff) in the event of an outbreak (containment)
4. Be able to support any operating system and computing device a student may bring to school
5. Prevent worm/virus DoS based outages

Determining the solution

The ASIS International Guidelines

In determining my recommendations for increasing the security posture of the Universities network, my first job was to determine what needed to be protected and at what cost. This necessitated a risk analysis of potential threats to cost of

[8] Livingston, Brian **How Long Must You Wait for an Anti-Virus Fix?**
URL:http://www.esecurityplanet.com/views/article.php/3316511
[9] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford and Nicholas Weaver, **The Spread of the Sapphire/Slammer Worm**
URL: http://www.caida.org/outreach/papers/2003/sapphire/

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

countermeasures. For determining what must be done, I used the General Security Risk Guideline by ASIS International[10]. This guideline breaks security risk assessment down into 7 steps, which gives a solid methodology for determining if a particular risk justifies the cost of a particular countermeasure. In the end it doesn't make sense to purchase $100,000 worth of security to protect something with a value of $1000 dollars.

Step 1 Understand the organization, the people, and assets at risk.

The IT group of the University had a limited budget and a small staff. Any event that requires additional staff or expertise means that the IT group has to bring in outside consultants to assist in mitigation. The assets that are at risk are pretty straight forward from a network standpoint, in that the 20 or so servers that run the core "business" of education must be secure. These servers were brought to a standstill with the MSBlaster attack and caused a significant interruption in service. E-mail was also taken off line which prevented the delivery of class information and correspondence between students and faculty. The other asset that was impacted drastically was the Internet connection. The internet connection was pulled for a few days while IT tried to figure out what was going on. This denial of service was a major inconvenience for everyone involved.

Step 2 Specify loss risk events/vulnerabilities.

The main source of risk for the University is with un-patched and vulnerable software. Over the past year they had to combat every major outbreak not only on the administration side, but also on the student side. Viruses and worms were not the only issues they had to face. Spyware and other malicious code were showing up on student computers and labs requiring manual removal or re-imaging. Resource exhaustion was also shown to be a major vulnerability. No bandwidth limiting was being utilized on student segments to prevent infected devices from utilizing all of the available bandwidth to propagate the infection. The wireless network was also considered vulnerable because of the lack of controls in place to prevent unauthorized access.

Step 3 Establish the probability of loss risk and the frequency of events.

The number of major outbreaks has been rising every year, as are the number of vulnerabilities found in software. This led us to assume with a strong degree of

[10] ASIS International **General Security Risk Assessment Guidelines** URL:http://www.asisonline.org/guidelines/guidelines.pdf

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

certainty that the likelihood of infection happening again was virtually assured. The frequency of major events that the IT group determined they had been required to manually intervene (where patching and/or anti-virus had not stopped it) was roughly 4 times in a year.

Step 4 Determine the impact of the events.

The impact was both monetary and physical for the IT group. They were all salaried, so there was no overtime. IT salaries averaged $50 an hour x 4 employees. Cleaning up the effects of the outbreak consumed 2 weeks or 80 hours which cost the University $16000. They had 3 consultants making $150 an hour to assist them in stemming the tide of the infection. These individuals worked 3 days x 8 hours a day. They cost the University over $10,800 in labor alone. Productivity at the university was greatly affected in that they had to carry out registration on paper until the network was back in service. This meant they had to re-enter all of the changes and class schedules from paper back to computer, which consumed a number of days of administration support wages. They estimated the cost at roughly $55000 in wages and lost productivity, because the University was virtually at a standstill for a number of days. On the intangible side of things, the physical impact of these long days took their toll on the IT group, and moral was affected. The President of the university was also very interested in hearing from the IT manager how this had happened as well as how it would be prevented in the future.

Step 5 Develop options to mitigate risks.

There were many ways to accomplish the goals that the University was working towards, and a number of potential solutions were discussed. Considering the fact that the University was primarily a Cisco shop, and had strong levels of experience and trust with Cisco products, it was considered a requirement to look at Cisco solutions to provide the options for mitigating the risk that we identified.

IDS

Cisco IDS was one of the first topics discussed as it was viewed as a mechanism to observe the security of the network from a packet standpoint. IDS was considered a good solution to give them visibility into the student segments as well as monitoring attacks and attempted attacks coming from the inside and outside of the network. The visibility into the network was identified as sorely missing for the IT department. How could they feel confident that things were okay on the network if they had no ability to look for unusual events? Cisco IDS would also give them the ability to have automatic response capabilities for packets viewed as malicious. The IDS sensor could configure automatic vlan access control lists (VACLs) to block the offending IP address and effectively

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

shut it off from the rest of the subnet and network. Since IDS was not dependent on client type, it was considered as a good way to provide security for the otherwise difficult to secure student segments of the network. The University decided to look at a way to leverage the investment in their core Catalyst 6500 switch by installing a Cisco IDSM2[11] blade in an empty slot. This blade would provide them with 600mb of sensing capabilities, which given their network and bandwidth utilization was deemed enough for a start. They also were interested in having a separate standalone appliance for the wireless segments that was configured with a much more aggressive sensing policy to look for malicious activity on those vectors of attack. The Cisco IDS 4215[12] appliance fit the bill. At 80mb of sensing capabilities, it would do a good job at monitoring the wireless segments.

CSA

Cisco Host based intrusion prevention was examined as a good candidate for preventing the day zero attacks that had plagued the university. The thought of trying to outfit every computer on campus (students and faculty) was considered to be financially taxing and administratively impossible. This led to the Idea of just focusing on the servers and key desktops. Lab computers were easily re-imaged in the event of an infection, and the IT group felt that they were not as critical as the 500+ faculty and support staff PC's that was used for the business functions of the school. Cisco Security Agent (CSA) was selected to provide this protection as well as to increase the level of policy control on the desktops themselves. Cisco was considered to have the only complete solution on the market by providing a behavior based Host Intrusion Detection System (HIDS) agent, a File Integrity agent, a Distributed Firewall, malicious code sandbox, and an NT audit log consolidation agent.[13] The agent also protects systems that have not been patched from attacks. This would allow the IT group to slow down the patch cycle until a better tested service pack or roll up patch was released. Patching could also be preformed in maintenance windows, as opposed to emergency patches during the day. This would increase server up time and make patching a much more cost effective activity. While CSA met the immediate need of preventing infection and alerting staff of security events, it also had the side benefit of helping with preventing the download and execution of applications from the internet. This could also prevent the installation of dialers[14] and spyware[15], which was another area that IT was having a tough time with.

[11] Cisco IDSM2 blade for Catalyst 6500 URL:http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html
[12] Cisco IDS 4215 Appliance URL:http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/ps5367/index.html
[13] Cisco CSA URL:http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html
[14] Dialer, Spyware-Guide URL:http://www.spywareguide.com/category_show.php?id=8
[15] Spyware, Webopedia URL:http://www.webopedia.com/TERM/s/spyware.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Cisco VMS

A solid security management application was sorely missing and the last thing IT wanted was to individually manage multiple devices and leave the integration to the individuals that had to interact with them. They wanted a solution that would provide status reports and correlation of events to determine the security health of the network, coupled with a single configuration tool. Since they were an all Cisco shop, it made sense to look at Cisco's VMS (VPN/Security Management Solution)[16]. This platform provided the ability to manage and monitor all of the security products that Cisco offered in a modular format. If you had a Firewall, you could add the management console for Firewalls. IDS? No problem, install the management console for IDS. The suite of applications also included an app called Security Monitor. This tool gave log collection capabilities as well as the ability to identify the events seen by all of the Cisco security products in production on the network. IT was very pleased to see a single interface to monitor all of the different products, as man power was tight and hiring specialized staff was not possible.

Router ACLs

Another option that was brought up did not require the purchase of any additional products or technologies to implement. The recommendation to create access control lists to limit connectivity to key servers to only the ports and services necessary was also added to the list. This is simply good practice in any organization, as it limits the potential misuse of a core server to the least applications as possible. Disabling unneeded services was also recommended as those services posed a risk for future vulnerabilities.

Step 6 Study the feasibility of implementation of options.

After careful evaluation of the mitigation options on the table, it was decided to work the solutions into a proposal to determine if they made sense and addressed the goals set forth during the initial problem identification phase.

The options on the table would have IT make the following changes to the network and security policy of the University.

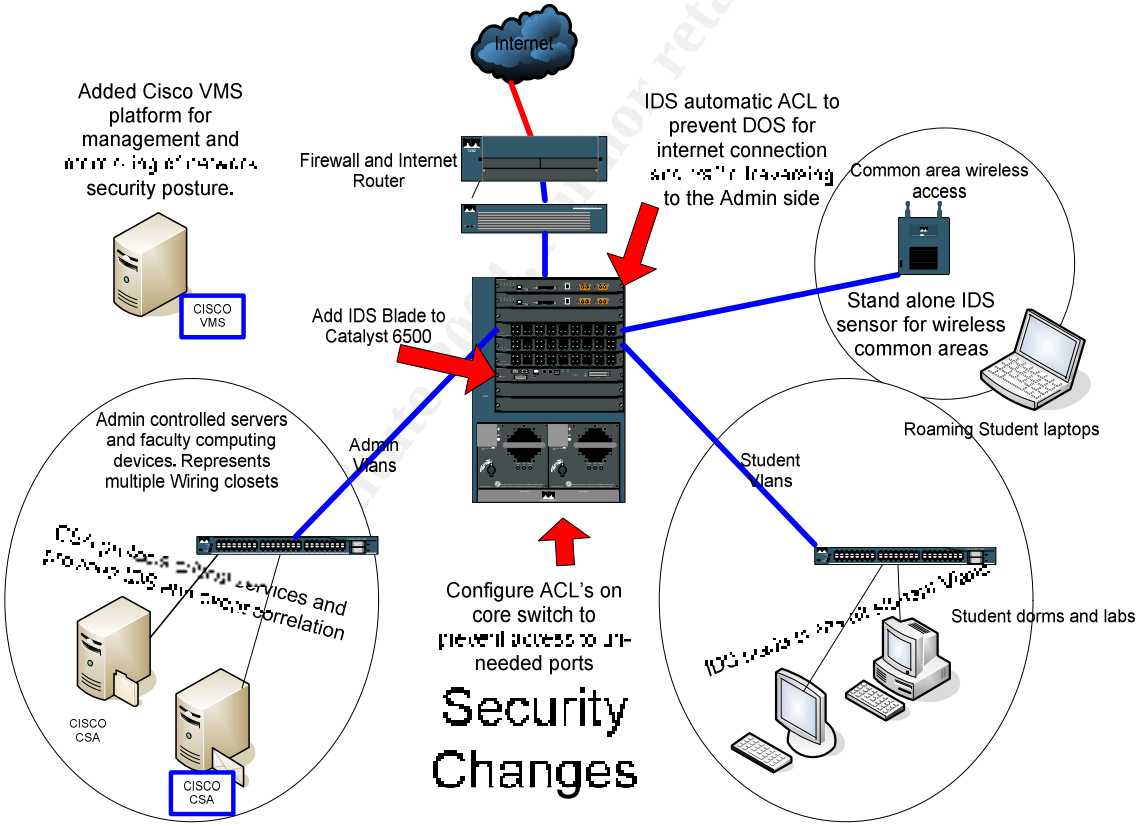
1. Deploy IDS for student vlans, and configure the IDS to automatically respond to known virus signatures to prevent the spread and re-infection of student computers. Configure the IDS to log and alert on misuse attempts by students above a certain threshold (ie. Alarm on attacks, password guessing, but not scanning). Configure IDS to automatically block offending computers until IT had an opportunity to evaluate and

[16] Cisco VMS URL:http://www.cisco.com/en/US/products/sw/cscowork/ps2330/index.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

educate the student on University misuse policies. Configure IDS to protect the Internet connection and access to the Administration segments of the network from Denial of Service.

2. Deploy Cisco Security Agent to protect key Microsoft Windows Servers and desktops. Configure the Agent to be as unobtrusive as possible by limiting user interaction with it. Prevent the download and execution of software on the university owned computers for average users, with “are you sure?” prompting for power users. Retain default security policy configuration until after the initial pilot.
3. Deploy Cisco VMS and configure it to monitor and control the IDS systems, Firewalls, and Cisco Security Agent. Configure automatic notification via e-mail and pager of serious events and automatically e-mail reports that detail the previous day’s security events and offending IP address to management.
4. Minimize unneeded services on university servers, and configure ACLs on the core switch to block access to all ports except for those required by applications.



Step 7 Perform a cost/benefit analysis.

The cost of these products versus the benefit was pretty obvious. The total list price of these solutions was roughly $100,000. This doesn’t include professional

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

services to implement it, but give a ball park cost of the additions to the network for the project.

The parts list included:
1 x IDSM2 IDS blade for the existing Catalyst 650
1 x IDS 4215 IDS Sensor for wireless common areas
600 x Cisco Secure Agent desktop Licenses
25 x Cisco Secure Agent server licenses
1 x Cisco VMS management application license

As previously noted, the IT department had incurred substantial cost with the outbreak of the MSblaster worm. This one incident is estimated to have cost the University a total of $81,800. While this number is an estimate, it really opened the eyes of the University board as to the risk they were taking by continuing on the same path as before. These numbers represent the tangible costs associated with the event, and do not take into account the impact these outbreaks can have on the customer, which in this case the is the University student. Loss of goodwill and trust toward the university can have drastic consequences. Education is as competitive as any business and a lost customer is still lost revenue.

Some of the benefits these solutions provide are in the form of a return on investment for the features added. The IT staff estimated that 30-35% of their time was spent patching or answering support calls from users with virus's or spyware related issues. This was time taken away from other University projects and absorbed a large chunk of the manpower budget that IT was allocated. With The whole patching problem has been addressed many times before, but there are some interesting numbers that factored in to the return on investment for slowing down the patching pace. In an article printed in December 2003 by Information Security magazine the following patching facts were compiled. [17]

Patch Factoids

4 The number of patches Microsoft released for the SQL vulnerability exploited by Slammer. The fourth patch, released a month before Slammer appeared, finally fixed the vulnerability. (Microsoft)

6 Months between the discovery of the SQL vulnerability and the appearance of the Slammer worm. (TruSecure/ICSA Labs)

26 Days Time between the release of the patch for the RPC-DCOM Windows vulnerability and appearance of the Blaster worm. At one point, Blaster was infecting up to 2,500 computers per hour. (Symantec)

50 Percentage of all vulnerabilities left unaddressed 30 days after the release of software patches. (Qualys)

80 Percentage of exploits released within two months of a vulnerability's public disclosure. (Qualys)

[17] Saita, Anne Information security Magazine Dec 2003, **Persistently vulnerable software has enterprises searching for better remediation solutions.** URL:http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss288_art530,00.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

$475,000 Median vulnerability remediation cost -- including Patching -- per company. This includes hard, soft and productivity costs. (TruSecure/ICSA Labs)

A more direct example of the cost savings approach to reducing the number of patches is to look a formula on the cost per patch presented in the Feb 2004 issue of Information Security Magazine.

Cost calculation formula:
(Hours x Rate x Systems) + (Patch Failure% x (Hours x Rate x Systems)) = Cost to Patch[18]

So, given the average hourly wage of $50, with 1 patch taking and hour, for 600 systems we get roughly $30,000. Let's also add the assumption that 5% of the patches are going to fail and require an extra 2 hours to fix the system or recover/re-image. This adds an additional $10,500 to the cost, with a grand total of $40,500 per patch. With the track record of major software vendors, it was assumed that a very large number of patches were going to be released in the coming months and years. Obviously this is a worst case scenario and with automated patch management solutions there are mechanisms to reduce the time in man hours by automating a good portion of this, but even the best automated patch management software still has problems. We saw with the previous patching fact bullets that not all patches fix the vulnerabilities the first time. While we did not assume that the Cisco Security Agent would allow the IT group to never have to patch again, it would give them the ability to slow the patch cycle down so that they could test patches or wait a little bit for a rollup patch. This takes a lot of the race out of patching and allows the IT group to patch within maintenance windows and not at the cost of productivity. The intrinsic value associated with a reduced patching cycle and the ability to stop subsequent outbreaks made it very clear to us that we had a solution that would justify the expense of the initial purchase. Comparing the cost of these products with the cost of an assumed 4 outbreaks a year and many, many patches, we were able to achieve an asymmetrical investment to savings (small investment achieves large gain) ratio for our security solution. If the average company has a potential vulnerability remediation cost of $475,000, the potential savings are pretty staggering when considering the cost of the solutions proposed. Even if you believe that number is 2x larger than it should be, we still have a nice 2-1 ratio for benefit-cost.

The Solution in Action

It took a couple of months to fully outfit the university with the complete solution, as budget was a concern. The VMS management application and the IDS sensor

[18] Lindstrom, Pete Information Security Magazine Feb 2004 **A Patch in Time** URL:http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss326_art580,00.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

went into place first. The benefits of these products were immediate in that the IT group could now see the posture of the network and view infected systems very quickly. The time it took them to find and remedy the infected systems was cut dramatically and the automatic blocking that the IDS sensor preformed on the offending device protected the rest of the network. This blocking also caused the student to call IT, because they no longer had access to the network. IT was then able to have the student bring there machine to them for virus/worm cleaning. In the first week of use the IT group had reports and graphs showing a lowering trend of infected machines.

Once CSA was deployed on the administration systems they had the opportunity to see it in action during a real world event. About 20% of the clients had the agent loaded and the rest were in process. Around this time the first versions of Beagle[19] and Netsky[20] were starting to circulate. This allowed the university to see the value of the security countermeasures by seeing them in action. CSA stopped the infection on the admin desktops, but the desktops without protection were hit. The IDS system was able to contain the infection on the student side and protect the network from being hit with a denial of service from the worms propagating. Ultimately there is no better test of a system than to see it do what it was intended to do. The IT group accelerated there deployment and finished in time to watch as a string of virus and worms were released between March 2004 to June 2004. CSA stopped every one.

Conclusion

Security is a series of tradeoffs between risks we are willing to accept and the threats that can do serious damage to our business. Budgets and people constraints in many ways force our hand in determining the solutions we implement to protect the most critical systems in our environments. If you follow a systematic plan that addresses the vectors of attack with the inherent value in dollars and criticality a system has to your organization, you will be able to make a much more informed decision as to where to place those dollars for countermeasures that will truly give you the best bang for the buck.

[19] Beagle url:http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.a@mm.html
[20] Netsky url:http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.d@mm.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

1) Webopedia URL:http://www.webopedia.com/TERM/M/malware.html (August 2004)

2) CERT/CC Statistics 1998-2004 URL: http://www.cert.org/stats/cert_stats.html (August 2004)

3) Nmap URL:http://www.insecure.org/nmap/ (August 2004)

4) Nessus URL:http://www.nessus.org/ (August 2004)

5) Mcafee URL: http://www.mcafee.com/us/ (August 2004)

6) SANS Internet Storm Center MSBlaster, 11 August 2003 URL: http://isc.sans.org/diary.php?date=2003-08-11 (August 2004)

7) Bowers, Tony "Lock IT Down: Antivirus software alone is not enough protection," Techrepublic 28 January 2004 URL:http://techrepublic.com.com/5100-6313-5140210.html (August 2004)

8) Livingston, Brian "How Long Must You Wait for an Anti-Virus Fix?" E-security Planet 23 February 2004 URL:http://www.esecurityplanet.com/views/article.php/3316511 (August 2004)

9) David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford and Nicholas Weaver, "The Spread of the Sapphire/Slammer Worm" 2003 URL: http://www.caida.org/outreach/papers/2003/sapphire/ (August 2004)

10) ASIS International "General Security Risk Assessment Guidelines" 2003 URL:http://www.asisonline.org/guidelines/guidelines.pdf (August 2004)

11) Cisco IDSM2 blade for Catalyst 6500 URL:http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html (August 2004)

12) Cisco IDS 4215 Appliance URL:http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/ps5367/index.html (August 2004)

13) Cisco CSA URL:http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html (August 2004)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

14) Dialer, Spyware-Guide
URL:http://www.spywareguide.com/category_show.php?id=8 (August 2004)

15) Spyware, Webopedia URL:http://www.webopedia.com/TERM/s/spyware.html (August 2004)

16) Cisco VMS
URL:http://www.cisco.com/en/US/products/sw/cscowork/ps2330/index.html (August 2004)

17) Saita, Anne Information security Magazine Dec 2003, "Persistently vulnerable software has enterprises searching for better remediation solutions." URL:http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss288_art530,00.html (August 2004)

18) Lindstrom, Pete, "A Patch in Time", Information Security Magazine Feb 2004 URL:http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss326_art580,00.html (August 2004)

19) Beagle
url:http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.a@mm.html (August 2004)

20) Netsky
url:http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.d@mm.html (August 2004)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced