Global Information Assurance Certification Paper

Introducing Information Security to a Cyber Café

A Case Study

GIAC Security Essential Certification (GSEC) Practical Assignment
Version 1.4b Option 2

Submitted by Barry A Basselgia
Date January 5, 2004

Introducing Information Security to a Cyber Café

Abstract

Due to growing concern over Information Security, I was approached by the director responsible for a company sponsored Cyber Café to evaluate the Café for Information Assurance and Network Security concerns. The director was concerned that a virus or other forms of cyber attack could cause extended downtime, which would have a negative impact on morale and productivity.

As it turned out, the week before I started my assessment threats were received via email. Law enforcement agencies were notified and the source of the emails was tracked back to one of the Cyber Café Locations. The Law enforcement agencies shut down the Cyber Cafés for 2 days during the investigation. Due to the non-existence of security policies at the Cyber Café, it could not be determined who specifically sent the email. This incident did get the attention of upper management, which made getting approval for most of the recommendations much easier.

Assessment

There are actually 3 locations that fall under the Cyber Café umbrella. The primary location, known as ECC, consists of 30 workstations and is open 24 hours a day. The second location is inside a food service outlet known as CPC. This location consists of 10 workstations and is open from 1100-2200 daily. The third location is in the library. This location consists of 2 workstations and the hours vary.

The Cyber Cafés are located in a very remote location. The nearest computer/electronics store is 7 hours away. Nearly 100% of the local population is either a company employee or works for a contractor supporting company operations. There is a small telephone company that services the area and provides ISP services. The charge for Dial-up Internet access is $.05 per minute. Long Distance phone calls start at $.50 per minute; due to the remote location all extra-company calls are long distance. The Cyber Café offers free Internet access and is the main form of communication between the employees and their friends and family. The availability of these Cyber Cafés has a direct impact on morale and employee productivity.

Current Policies

As stated above, there were no Information Assurance policies in place at the Cyber Cafes. The only thing even resembling a policy were stickers that were

placed on each monitor letting everyone know they were not allowed to download or print pornographic material.

Employee Interviews

The director indicated there were 2 major complaints from the Cyber Cafés. The first complaint was the inconsistent configuration of the workstations; no 2 workstations had the same software installed. The second complaint was the amount of time that many of the workstations were down; usually because virus infections or improper installations of unauthorized software.

There are 2 Technicians that are responsible for maintaining the workstations. Although, they had some knowledge of Information Security practices, they had no training and did not know were to start.

In addition to the Technicians, there are a number of "Attendants" that are responsible for maintaining a hand written log of who is using the computers and enforcing a 30 minute, computer use time limit. The attendants have no computer training.

A review of the usage logs indicated that at least 1000 employee's used the Cyber Cafés on a regular basis.

Physical Security

At the ECC, the DSL modems and hubs were sitting on an open shelf in a small office. The office was unlocked most of the time. There were long periods of time when no one was around the office.

At the CPC and library, the DSL modems and hubs were sitting on the tables next to the rows of workstations.

The Workstations

An examination of a random selection of the workstations revealed the following

- All of the workstations were running Microsoft Windows 98.
- No User-ID/Passwords were required.
- There was a simple timer program being used to limit each person to 30 minutes. The Users had figured out that they could defeat the usage timer by changing the system clock. Every workstation was set to a different date/time.
- Anti-Virus software had been installed, but was disabled on many of the workstations and the virus definitions were not current
- Un-registered shareware and bootleg software were also found.

- Kazaa had been installed on some of the workstations and was being used to share bootleg music files and software.
- The Sub-Seven Trojan was found on a number of workstations.

Network Architecture

Internet connectivity is provided from the local ISP to each of the Cyber Café locations via DSL lines. The ISP does not provide any firewall or security services.

The ECC has 2 DSL lines; the workstations are divided equally between these 2 lines.

The CPC and Library each have their own DSL line.

Assessment Conclusions

At this point it was quite clear that running any security scanning tools would have been a waste of time. The Cyber Cafés were going to have to be re-built from the ground up.

Recommendations

After completing the above assessment I consolidated my findings and made the following recommendations.

1. Policies and Procedures

Policies are the keystone to any Information Assurance program. The company already had in place effective Information Assurance policies. Although the Cyber Cafés are not part of the company network, the workstations are company assets and should, with a few exceptions, follow company policies. At first glance the following company policies could be applied directly to the Cyber Café:

1. The policy and procedures regarding authorized software. This policy includes:
    a. What operating systems are authorized
    b. What application software is authorized
    c. How to get new software added to the authorized list.
    d. The proper installation of operating systems and application software.
    e. The proper installation of service packs, security updates and hot fixes.
2. The policy and procedures regarding anti-virus software.

3. The policy and procedures regarding User-ID's and passwords.

Other company policies may also be applicable. One policy that would need to be modified for the Cyber Café would be the acceptable use policy. This may be obvious to some, but what the company would find as acceptable use on a workstation in a work center would not necessarily be the same thing they'd find acceptable from the Cyber Café.

2. Employees

The Technicians are capable of implementing the policies and procedures, once they are established.

Any Employee wishing to use the Cyber Cafés would have to be issued a user-id/password and sign a user acknowledgment stating they understood the acceptable use policies for the Cyber Cafés.

3. Physical Security

At the ECC, a lock should be placed on the office were the network equipment is located. Access to this office should be limited to the authorized personnel only. Materials located in this office that are used by un-authorized personnel should be relocated.

At the CPC and Library, a wall mounted rack or cabinet with a lock should be installed for the network equipment.

4. Workstations

In accordance with the before mentioned policies, all workstations would have to be upgraded to Windows 2000. The appropriate service packs, security updates, and hot fixes would also have to be installed.

The company already has a corporate license for Symantec Anti-Virus Corporate Edition; detailed information on this product is available at http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155. Because this product provides central management and auditing features, it was recommended that this package be installed on all workstations and maintained in accordance with the already existing company policies.

Additionally, the following software not currently on the authorized list should be approved for use in the Cyber Cafés.

1. Instance messaging software (i.e. Yahoo, MSN)
2. Internet Portal software (i.e. AOL, MSN)
3. News group reader application

4. Internet relay chat application

Users should be required to logon to the workstations with a user-id and password.

5. Network Architecture

In order to provide for central management of the workstations, the purchase of a Windows 2000 server was recommended. Windows 2000 Active Directory would provide user authentication and allow the implementation of policies on all the workstations.

The purchase of a LINKSYS DSL Firewall/Router with VPN capabilities was recommended, detailed information on this product is available at http://www.linksys.com/products/product.asp?grid=34&scid=29&prid=433 . This would provide basic protection from outside attacks while allowing the separate locations to be managed and monitored, from a central location.

A second windows 2000 server was also recommended to run as a proxy server using Microsoft's ISA server, detailed information on this product is available at http://www.microsoft.com/ISAServer/ . The web caching features of this product would provide more efficient use of the available bandwidth. This product also offers additional security features if the need for a more robust firewall arises in the future.

6. Legal Liabilities

The legal liability the Cyber Cafés present to the company was demonstrated both by the occurrence email threats and Kazaa file sharing that was going on. The purchase of CyBlock Web Filter from Wavecrest Computing was recommended, detailed information on this product is available at http://www.cyblock.com/products/cyblock/index.html. CyBlcok categorizes web sites into 55 standard categories. Working with Microsoft's ISA server allows the blocking of websites based on these categories. The control files are updated on a weekly basis and are downloaded automatically by the application.

7. On Going Monitoring

Information Security is not a "once and done" proposition. Baseline security measures should be established during the implementation of the above recommendations. A part-time Information Security Specialist/Consultant should be hired to monitor the Information Security State of the Cyber Cafés and make adjustments and additional recommendations as needed.

Implementation

All of the above recommendations were approved.

A few factors were going to make implementation tricky.

1. The remote location meant that any new equipment being purchased would take 3 to 6 months to arrive.
2. Down time at the Cyber Cafés had to be minimized.
3. Because of the direct relationship the Cyber Cafés had to employee morale and productivity. Impact to the users had to be kept to a minimum.

Keeping these factors in mind it was decided to implement the changes in 3 parts. Because of its size and operating hours, the ECC location was determined to present the biggest risk and was our initial target. The lessons learned from upgrading the ECC would then, hopefully, make upgrading the other locations go more smoothly.

Part 1 - Introducing Network Security to the ECC

The upgrades would be done in phases as the equipment arrived.

ECC Phase 1

Because we didn't want to wait 3 to 6 months for all the equipment to get here, we started on the things we could do with items on hand. The company did have available licenses to upgrade the 30 workstations to Windows 2000. An older server was made available on a temporary basis to get us started.

Building a Server

A fresh installation of Windows 2000 Server was performed on the server. Service Pack 4 was installed and Windows Update was used to install the current hot fixes. "Securing Windows 200 Server" by Cory Bys from the SANS Reading Room http://www.sans.org/rr/papers/index.php?id=189 was used as a guide for securing the server

The server was made an Active Directory Domain Controller. DNS services were established on this server with the zone information integrated into Active Directory. As there were no other DNS servers, the service was configured not to perform zone transfers.

Symantec Antivirus Corporate Edition was installed on the server. Client configuration options were set in accordance with the established policies. The server was also configured to download the current virus definitions on a regular schedule and push them out to the clients.

Since this server was not going to be a web server, IIS and other un-used services were either un-installed or disabled.

A share point was established as an installation point for the client software that had been authorized. Permissions were established on this share point so that only the technicians could access it.

Microsoft Baseline Security Analyzer (MBSA) was installed and run against the server to verify that all the appropriate security updates had been installed. Information regarding MBSA can be found in Microsoft Knowledge Base Article 320454 http://support.microsoft.com/default.aspx?scid=kb;en-us;320454. To our surprise we found that although Windows Update indicated we had all the current hot fixes. MBSA indicated some were missing. Availability of the missing hot fixes were verified and subsequently installed.

The Center for Internet Security's (CIS) benchmarking and scoring tools, available from http://www.cisecurity.org/ , were also run to establish baseline measurements that could be used for comparison in the future.

Upgrading the workstations

Training was held with the Technicians to ensure they understood the procedures for properly installing Windows 2000 Professional, Service Pack 4, and the current hot fixes. "Building a Secure Windows 2000 Professional Network Installation" by Bruce Fyfe from the SANS Reading Room http://www.sans.org/rr/papers/index.php?id=218 was used as a guide.

The Technicians then installed Windows 2000 Professional and all the authorized client applications on 5 of the workstations.

Symantec Antivirus Corporate Edition was pushed out to the 5 workstations from the server. The clients were automatically configured with the policies set on the server and virus signature updates would be pushed out as they became available.

MBSA was used to scan the workstations to verify that all the security hot fixes had been installed. The same discrepancies between MBSA and Windows Update were found and the appropriate hot fixes installed.

The CIS benchmarking and security tools were also ran to establish baseline measurements.

We allowed these workstations to be used for a week. Very few problems were reported and the technicians were able to easily correct them all. Most of the

problems stemmed from the users not being familiar with the Windows 2000 environment.

After the first weeks testing and evaluation, the Technicians installed Windows 2000 Professional on the remaining workstations. Additionally, Symantec Antivirus was pushed out, MBSA was run and CIS benchmarks were established.

End User Comments

We did receive a few comments from some of the end users. Most of these were positive. Users felt the systems were running faster and were more reliable. A few complaints were made because of software that was no longer available on the workstations and could not be re-installed by the end user. When these users were informed of the procedures for requesting new software, they withdrew their comments. The other complaint we received was about the workstations being bombarded with pop-up ads and messages. This issue would be dealt with later on.

Initial Network Monitoring

Network monitoring was conducted using Network Sniffer Packet Analyzer, available from Javvin Company; detailed information on this product is available at http://www.javvin.com/packet.html. This allowed us to analyze the traffic to and from our network. Using this tool we were able to detect that some of our users had managed to get Kazaa reinstalled on some of the workstations. The technicians removed Kazaa and the users were issued a warning.

Symantec Antivirus audit logs also revealed a few cases of people trying to download hacking tools and bootleg software. Most of these tools were infected with viruses. Law enforcement authorities were notified and investigations are underway.

ECC Phase 2

The routers/firewalls were received and installed on the 2 DSL lines at the ECC. The firewall capabilities of the router were enabled. The NAT and DHCP features were also enabled. The workstations were reconfigured to use DHCP.

A VPN connection was established between the 2 DSL lines, joining all the systems onto one network.

From the users point of view, the most evident result of the firewall being in place was that they were no longer getting the pop-up ads and messages.

We also setup the Multi Router Traffic Grapher (MRTG) to monitor our bandwidth utilization. MRTG was written by Tobias Oetiker and Dave Rand and is available

at http://people.ee.ethz.ch/~oetiker/webtools/mrtg/ . It can be used to collect and graph data from any SNMP manageable device. The SNMP features of the routers were enabled and the default community strings were changed. One of the features of the router/firewall is that it won't respond to SNMP requests from the WAN port. This made the risk from SNMP vulnerabilities low. MRTG uses a web-based interface to present its graphs. IIS was installed on the server. The server was checked to ensure the current security patches were installed and was configured to only respond to request from the local network. Once a baseline was established. It became apparent that we were not getting the bandwidth our ISP was supposed to be providing. All the graphs were flat lining at 256kbps. Our DSL lines were suppose to be providing us at least 512kbps. We contacted the ISP and they discovered that the DSL modems on their end had a configuration error; the ISP corrected the problem.

The router/firewall also had syslog capabilities. Since Windows 2000 doesn't have a syslog feature, Kiwi Syslog Daemon for Windows was installed on the server. Kiwi Syslog Deamon for Windows is available from KIWI Enterprises at http://www.kiwisyslog.com/products.htm#syslog. The router/firewall was configured to log events to the server. Review of the logs verified that the firewall was blocking unwanted traffic and provided us our first look at what websites our users were visiting. As it turned out, the warning sticker mentioned earlier regarding accessing pornographic sites wasn't having much impact. The syslog daemon has the ability to send alerts when specific events are logged. We developed a simple keyword list to identify possible pornographic sites. When an alert was generated we would approach the user and remind them that they were violating the policy regarding accessing pornographic material. Unfortunately, there was in fact no written policy regarding accessing pornographic material. Taking suggestions from "Network Security for Dummies" by Chey Cobb; chapter 4 and "Planning and Implementing Security Policies and Procedures and Information Security Policies, Procedures, and Standards"; by Thomas R. Peltier, a policy was drafted and submitted for approval via the companies' legal offices.

ECC Phase 3

The Servers were received and Windows 2000 was installed on them using the same procedures discussed earlier.

The first server was setup as a Windows 2000 Active Directory domain controller. This server was placed on the other side of the VPN connection, which greatly increased the speed of the logon process.

The second server had Microsoft's Internet Security and Acceleration (ISA) server installed and was configured as a proxy server/web-cache. Using "Windows 2000 Group Policy, Profiles, and IntelliMirror", by Jeremy Moskowitz, chapter 2 Windows 2000 ADM Templates as a reference, an Active Directory group policy was established to configure Internet Explorer to use the ISA server.

The performance of the ISA server was monitored and setting adjusted using it's built in monitors. The CyBlock package was then installed on the server. The CyBlock package has built in reporting capabilities. Upon reviewing the reports, we discovered that many more of the users then we thought were accessing pornographic sites. We are still waiting for the Legal Office to approve the policy that was submitted. At this point all we can do is monitor the situation. We consider this to be a potential security issue, because the anti virus logs indicate that a large number of the viruses being detected are coming from pornographic sites. This was obvious from the filenames involved. Furthermore most people would not report a virus if the source of the virus was a porn site they shouldn't have been browsing in the first place.

ECC Phase 4

A new electronic combination lock was placed on the office door at the ECC; only authorized personnel were given codes to the lock. Work orders have been submitted to remodel a storage area for the Technicians and Attendants to use as a work area. This will allow the office to be used solely for the servers and networking equipment.

Parts 2 and 3 – The CPC and Library

The holiday season is currently upon us.. We should be moving onto parts 2 and 3 after the New Year.

Post Assessment

Part 1 has been finished now for about 2 months.

There has been no downtime due network security issues.

Although the Anti-Virus software has detected a number of viruses, none of the workstations have actually been infected.

Auditing done with MSBA and CIS benchmarking and scoring tools indicates the technicians are following the policies regarding keeping the systems updated with current hot fixes.

System monitoring has detected a number of attempts to download hacker tools and bootleg software. These attempts have been reported to the appropriate law enforcement agencies and investigations are underway. Feedback from the law enforcement officers indicates they are very pleased with the amount of information we are able to provide them.

We are still waiting for the legal office to approve our policy concerning pornographic sites. We continue to monitor and generate reports on this activity but have not been given the authority to use the blocking features of the CyBlock package.

Overall feedback from the users indicates they are pleased with the changes, Internet access is faster, and the workstations are more reliable.

Company management is very please with these results. They feel that a good balance between Information Security, Limiting the Companies Legal Exposure, and providing a place for employees to relax, have fun and communicate with friends and family has been achieved.

References

SANS Security Essentials with CISSP CBK, Volume One, by Eric Cole, Jason Fossen, Stephen Northcut, and Hal Pomeranz

SANS Security Essentials with CISSP CBK, Volume Two, by Eric Cole, Jason Fossen, Stephen Northcut, and Hal Pomeranz

Network Security for Dummies, by Chey Cobb, from Wiley Publishing, Inc

Information Security Policies, Procedures, and Standards, by Thomas R. Peltier, from Auerbach Publications

The Complete Idiot's Guide to Internet Privacy and Security, by Preston Gralla, from Pearson Education, Inc

Building an Information Security Awareness Program, by Mark B. Desman, from Auerbach Publications

Windows 2000 Group Policy, Profiles, and IntelliMirror, by Jeremy Moskowitz, from Sybex Inc

Securing Windows 200 Server by Cory Bys from the SANS Reading Room http://www.sans.org/rr/papers/index.php?id=189

Building a Secure Windows 2000 Professional Network Installation by Bruce Fyfe from the SANS Reading Room http://www.sans.org/rr/papers/index.php?id=218

Symantec Anti-Virus Corporate Edition, detailed information on this product is available at http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155

LINKSYS DSL Firewall/Router with VPN detailed information on this product is available at http://www.linksys.com/products/product.asp?grid=34&scid=29&prid=433

Microsoft's ISA server, detailed information on this product is available at http://www.microsoft.com/ISAServer/

CyBlock Web Filter from Wavecrest Computing, detailed information on this product is available at http://www.cyblock.com/products/cyblock/index.html .

Microsoft Baseline Security Analyzer (MBSA) information regarding MBSA can be found in Microsoft Knowledge Base Article 320454 http://support.microsoft.com/default.aspx?scid=kb;en-us;320454

Center for Internet Security's (CIS) benchmarking and scoring tools, available from http://www.cisecurity.org/

Network Sniffer Packet Analyzer, available from Javvin Company http://www.javvin.com/packet.html

Multi Router Traffic Grapher (MRTG) written by Tobias Oetiker and Dave Rand and is available at http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

Kiwi Syslog Daemon for Windows, available from KIWI Enterprises at http://www.kiwisyslog.com/products.htm#syslog

Last Updated: July 23rd, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	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 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
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
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 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 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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor