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 (Security 401)"
at http://www.giac.org/registration/gsec

Gene LeDuc
GSEC Practical version 1.4b
Taking a Small Non-Profit Organization from Dial-up to Broadband

Abstract

Internet Access has become a mission critical part of nearly every business and nonprofit organization, regardless of size. The size and complexity of e-mail, web sites, e-commerce and online databases now require faster access methods than dial-up modems can provide. Even the fastest dial-up standards available today, or proposed for the near future, are too slow for the large e-mail attachments and graphics-rich web sites of today. The most cost-effective solution for many small organizations has become Digital Subscriber Lines (DSL) or Cable Modems. Although delivering a welcome bandwidth increase, the downside to these types of always-on connections is increased risk of attack and increased need for effective security measures.

This paper will provide a case study of the upgrade of a small non-profit organization's office from several stand-alone PCs using dial-up 56k to always-on broadband DSL Internet access. It will then review the resulting infrastructure in terms of desired security and whether the needs of the office were met. Finally, it will look at the impact of the upgrade on the organization's users, business productivity, and security. The period of time covered by this paper is approximately 3 months.

Before

I am a volunteer for a non-profit organization I will call NPO. Although NPO has affiliates and volunteers worldwide, it is administratively small and operated from a 2-office suite in Southern California. There are 2 paid employees, an Office Manager and an Office Assistant. The level of computer and network knowledge at the NPO office is very low. Nearly all technical questions are directed to me and once or twice a year I make a 250 mile house call to their office to make sure that everything still looks good and that everyone is still able to work with their computers. NPO's office budget is minimal and provided by seminars presented by NPO volunteers.

NPO's pre-broadband network infrastructure consisted of the following:

- 2 e-mail addresses provided by 1 America Online (AOL) account
- a web site at a hosting company
- dial-up internet access for 2 PCs via the AOL service (only 1 could be online at a time)
- 2 stand-alone PCs, one with a laser printer and the other with a color inkjet printer attached locally

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- 1 dedicated PC hosting a custom Integrated Voice Response (IVR) program for answering a toll-free phone number
- 1 server at a colocation facility used to host NPO's domain name server, a web server, an e-mail server and mailing list software

The staff and board of directors of NPO recognized that office productivity was being significantly degraded by the bottleneck of a single dial-up Internet connection. Incoming e-mail often contained large attachments that were to be uploaded to their colocation web server; this tied up one of the staff PCs for the time it took to download the attachments and then again to upload them to the web server. Only 1 of the 2 e-mail accounts could be accessed at a time and the cost of remaining online for hours/day with the dial-up connection had become too high. With the advent of widespread DSL the board asked me to look into upgrading the office to broadband Internet access.

My to-do list looked like this:
- Check availability and cost of cable and DSL service
- Inventory current computing assets
- Evaluate the needs of NPO's staff
- Propose new infrastructure to board of directors
- Purchase and install necessary hardware and software
- Evaluate whether needs of NPO's staff are met
- Evaluate security of the new infrastructure
- Examine and deal with non-infrastructure security issues

During

Check availability and cost of cable and DSL service
NPO's office was located close enough to the local telco central office that DSL was a viable option. Business DSL in the area was provided by the local telco and 3 other provider partners. Although cable was available in the area, it was not installed in the strip mall housing NPO's office and the cost and delay in getting it installed were considered a negative by the board. We chose a local DSL provider that partnered with the local telco to provide DSL service at a reasonable rate along with free technical support. The DSL provider gave us a single dynamic IP address, 10 e-mail boxes and authorization to connect multiple computers to the Internet via their DSL connection at no additional charge. They also provided a free DSL modem.

Inventory current computing assets
My next task was to make an inventory of all computer and network assets either at or controlled by the NPO office. Since we did not expect to make any changes to the desktop software environment I limited the inventory to actual hardware and software that functioned as part of the security program. Here's what I found:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- There were 2 PCs used by the staff. These ranged in age from just over 1 year to almost 3 years old. Because they were not presenting any problems we decided to keep them and look at them again in a year.
- There were 2 printers: a 1 year old HP LaserJet and a 2 year old HP color inkjet. The laser had an integrated print server, was fast enough, and met the needs of the office, so it went on the keep list. The color inkjet was slow and noisy, but it did produce reasonable output and was not used often enough to become annoying. We decided to keep both printers, but review the color inkjet in a year.
- The hosted web site had a large bandwidth and sufficient storage at a very low cost; we chose to continue to host our primary web site with the hosting company.
- The 2 e-mail accounts were considered to be acceptable for the short term, but we wanted to transition to addresses with our own domain within a year.
- The dedicated IVR PC was over 3 years old. We decided that we wanted to move the IVR program to a newer machine but discovered that it would only run reliably under Windows 3.x or Windows 95. We decided to buy a new PC to replace one of the staff PCs and move the IVR system (with Windows 95) onto the newer replaced PC.
- The 2-year old Linux server at the colocation facility hosted a number of low-traffic web sites, NPO's primary DNS server, mailing list software for supporting 13 lists and an e-mail server for NPO's domain. The server had plenty of disk space remaining, plenty of RAM, and the CPU utilization stayed consistently below 5% so we elected to keep it. We would revisit the option of replacing this server in 1 year.
- We had a 5-user license and a mail server license for anti-virus software with 2 years remaining on a paid upgrade subscription. We would keep the anti-virus software.

Evaluate the needs of NPO's staff

Since we were looking at a significant change in the infrastructure I wanted to also make sure that we would address the needs of NPO's staff, even those that we may not have known about before. I spent half a day watching how the staff conducted their daily routine and asking them about the various tasks and frustrations they dealt with on a regular basis. After discussing various possibilities, we resolved their computing needs to be:

- access the Internet to send and receive e-mail
- access the Internet to maintain content on several of the web sites
- access both printers from the 2 PCs and the dedicated IVR PC
- be able to share one of the PC's drives with the other PC
- be protected from attacks from the outside, especially viruses

Propose new infrastructure to board of directors

The new NPO infrastructure that I envisioned would be a small 100Mb ethernet LAN connected to the DSL modem via a SOHO firewall appliance. I wanted to

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

install a Linux server to act as an e-mail server and file server for the network. Although it was connected to a PC with a parallel cable, the laser printer already had an internal print server and was just waiting to be plugged into a network. I wanted to install an external print server on the inkjet to make it a network printer as well. NPO already had a 2-year upgrade subscription and sufficient licenses to run Sophos[i] anti-virus software on the PCs and the colocated e-mail server. The new Linux e-mail server would only be accepting mail from the protected colocation mail server, so I judged that the existing anti-virus package on that server would be sufficient and that the new Linux server could go without anti-virus protection.

I presented my suggestion to the board of directors via e-mail. There was some telephone discussion with the board chairman and office staff and it was finally decided to go with my proposal, but minus the file server portion of the Linux server. Each PC already had an internal tape backup system and this was considered more economical than installing a new backup system on the Linux server. I was given the go-ahead to buy the necessary software and hardware.

Purchase and install necessary hardware and software

I saw that the major purchase would be a new PC and a firewall appliance to keep intruders off of the network. Smaller purchases would be an external print server and various connection cables. I researched the firewall options by talking to representatives at local trade shows and then asking advice from a group of network security administrators that I meet with. I had already decided to go with a Dell Optiplex for the new PC based on my experience installing them at work.

- Firewall
  After talking to representatives of several firewall appliance companies and reading firewall reviews in various trade magazines I settled on the TELE-3[ii] firewall from SonicWall. The firewall is a modem-sized appliance that provides Network Address Translation (NAT) for letting up to 5 devices access the Internet using a single shared Internet address, 5 VPN tunnels, remote maintenance over via VPN or SSL, automatic e-mailing of logs and reports and good technical support. While the TELE-3 can't be upgraded to allow more than 5 internal addresses to access the Internet, this was not considered a problem as there is little likelihood of increasing the size of the office staff. Setup of this device is done via web browser and is very straightforward; the defaults would probably be sufficient for most small networks. The only changes I made were to allow e-mail from the external mail server through to the internal mail server and to allow SSH into the internal Linux server for remote maintenance. I also assigned IP addresses to the MAC addresses for the 2 print servers and the dedicated IVR PC and then restricted them from accessing the Internet. Restricting these 3 addresses from the Internet meant that these 3 would not count against my 5-address limit. The TELE-3 configured its network settings automatically by contacting the DSL provider's DHCP servers and then provided the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

appropriate network settings to all the network computers and printers via its own DHCP server. It even lets me know when a firmware upgrade is available.

- Network hub
  This is a small network with very modest utilization so I was satisfied with using a Kingston 8-port hub that was provided at no charge by a NPO volunteer.

- PC
  I chose to buy a Dell Optiplex GX-110 to replace one of the staff PCs. My choice of Dell was entirely due to my good experience with their reliability and great experience with their next business day repair policy. Since I live in another part of California, reliable support from the vendor was a must. The replaced PC's hard drive was slicked and I installed the latest version of Windows 95, along with the IVR software and hardware. The IVR PC was configured to use DHCP so it would be assigned an address that is blocked from leaving the network. The 2 other PCs also use DHCP, but their addresses are allowed onto the Internet.

- Print servers
  The HP laser printer already had an integrated ethernet print server so I only had to select an external print server for the inkjet. The laser's integrated print server uses HP's Jet Direct for configuration so I chose an external print server from HP to simplify the configuration. I configured the print servers to use DHCP so that they would get addresses from the firewall that were blocked from leaving the network.

- Linux server
  I installed the latest version of RedHat Linux on a Dell Optiplex GX-100 PC donated by a NPO volunteer. I installed and configured a POP3 server (qpopper) and an e-mail server (sendmail). The POP3 server will be used to provide e-mail service to the office PCs when NPO switches from AOL to their own domain for e-mail. All incoming e-mail will come in via the existing mail server on the colocated Linux server. The new Linux server uses DHCP to get its network settings from the firewall.

- Software
  We chose to use Secure Shell server for Linux and client for Windows from SSH[iii] because we could get a free non-commercial license. We also purchased a single Windows VPN client from SonicWall so I could maintain the firewall remotely without opening its SSL port to the Internet.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

After

Evaluate whether needs of NPO's staff are met
After installing the new hardware and working the bugs out of the network I trained the staff on the new features of their network. I configured one of the staff PCs and the IVR PC to share their drives and then showed the staff how to access the shares. Then I trained them on using the networked printers and accessing their AOL e-mail accounts over the new Internet connection.

After a month, I called the office to follow up on how the new network was doing and whether there was anything that they needed that we had forgotten to plan for. Everything was working as they expected and they were extremely pleased with the increased bandwidth to the Internet. We discussed advancing the timetable to shift the e-mail from AOL to our own domain. I also later decided that we should install battery UPS systems on all 3 PCs and the Linux server.

Evaluate security of the new infrastructure
Since installing the firewall and network, I've conducted several security tests against NPO's network from the outside. The software I've used to test the firewall include

- Nmap[iv] – a robust and free port scanner, one of the best available at any price
- Internet Scanner from ISS[v] – a commercial vulnerability scanner with a huge database of known exploits to probe for
- Nessus[vi] – a free vulnerability scanner, one of the best available

Nmap discovered that I had left the SSL maintenance port open facing the Internet, so I closed it. Other than this, I haven't been able to discover any chinks in the wall. In next year's budget I will propose hiring an outside security testing company to test our security more thoroughly.

The local power grid has turned out to be a significant security threat for NPO's office. The strip mall in which it is located has had 5 power outages in the past year. Fortunately, only 1 of the outages hit during working hours. Unfortunately, that outage resulted in loss of data. The battery UPS systems that I decided the office should have were postponed for budgetary reasons, but after the data loss we came up with the money to protect the 3 PCs and the Linux server with SmartUPS units from APC. The firewall is plugged into the Linux server's UPS along with the hub and DSL modem.

I've also found that it's useful to be able to get remote control access to the PCs. I briefly considered pcAnywhere but decided to use VNC[vii] instead because of price and the programs' memory and disk footprints. I've installed a VNC server on each PC and configured them with a different passwords known only to me. When I need to get into a PC remotely I use the SonicWall Windows VPN client

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

to open a secure tunnel through the firewall into NPO's network and then use VNC to connect to the PC using its local IP address.

While the security of NPO's office network seems to be sufficient, I've discovered that the external portion of NPO's infrastructure is at significant risk. The colocated server is attached directly to the facility's backbone via a DSL chokepoint (to limit bandwidth). Although the server has been hardened to some extent, and all the server software is up-to-date on patches, the software it is running has had recent vulnerabilities and there are bound to be more discovered. The next order of business for NPO will be to install a firewall at the colocation facility to protect their server. I will prioritize this to happen before we get an outside security audit so that both firewalls will be included in the audit.

Examine and deal with non-infrastructure security issues

The final part of the network installation was to address "soft" security issues, those that do not involve hardware. The following guidelines include some found on the SecurityFocus[viii] and Network Computing[ix] web sites and were chosen to make sure that the NPO staff does not ignore the obvious (to me) exploits.

- Wherever possible, Internet Explorer is removed. Netscape 4.79 is the current standard, though this may change as new browsers become stable. Netscape is configured to allow cookies to be sent only to the originating server and JavaScript is disabled for mail.
- Outlook Express is removed wherever possible. Mail is read with Netscape instead.
- Installation of unauthorized software on PCs is forbidden. I check for this when I conduct my periodic visits to the office.
- Active-X is disabled.
- Daily backup tapes are stored offsite and rotated weekly.
- The NPO office seldom has visitors, so the front door is kept locked.
- Windows Shell Scripting is disabled wherever possible.
- Staff is trained to avoid opening any attachments unless they can confirm that they were sent, on purpose, by known entities.
- Staff is trained to avoid clicking on any links contained in e-mail.
- Staff is trained to turn off JavaScript when they find themselves in Popup Hell, then close all the extra browser windows before enabling it again.
- File transfer and shell connections to NPO's external web server are by SSH only. This prevents exposure of authentication credentials and encrypts the entire transmission.
- Modified Windows registry to associate various dangerous extensions like REG and VBS files with notepad. This is a backup in case someone does click on one of these attachments or links.
- Staff is trained to refer all questions about the NPO network or computers to their IT specialist (me).
- Training has been provided about the dangers of social engineering, how to recognize it and what to do if it happens.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Staff updates anti-virus signatures on PCs when new signatures are available. Sophos provides an alert mailing list for this purpose.

Impact

Upgrading NPO's office from standalone PCs with dial-up to a LAN with broadband Internet access has had a profound impact on the NPO office and staff. Measurable improvements include

- Productivity: File transfers that routinely took 30-90 minutes now happen in a couple of minutes freeing staff to work on other projects.
- Productivity: Everyone can now access the Internet at the same time. This is a huge savings in time as users are no longer limited to checking and sending e-mail one at a time.
- Cost: the cost of the DSL connection is nearly offset by the cost of keeping a business phone line connected to the Internet most of the day. Once the switch from AOL mail is complete and AOL discontinued, the DSL connection may actually prove to be cheaper.
- Security: The firewall blocks about 100 probes or access attempts every day. With the dial-up connection up for most of the day, there were probably a number of probes that made it into the connected PC.

Intangible improvements include

- Morale: Users are much happier when they are able to get their e-mail right away rather than wait long periods of time for it to download.
- Confidence: Users feel more secure knowing that there is a firewall that is always on, blocking hundreds of probes and access attempts per day.

The entire upgrade process from start to finish took about 3 months. There were very few glitches and all new hardware and software installed and ran as expected. The security posture of NPO's network is vastly improved with the upgrade and the users are much happier. This project was definitely a win on all fronts.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

[i] "Sophos – anti-virus for business." URL: http://www.sophos.com/
[ii] "SonicWall TELE-3 product description." URL: http://www.sonicwall.com/products/tele3.html
[iii] "SSH Communications Security." URL: http://www.ssh.com/
[iv] "Nmap free stealth network port scanner." URL: http://www.insecure.org/
[v] "Internet Security Systems, Inc." URL: http://www.iss.net/
[vi] "Nessus security scanner home page." URL: http://www.nessus.org/
[vii] "RealVNC." URL: http://www.realvnc.com/
[viii] Chuvakin, Anton and Dunham, Ken. "Basic Security Checklist for Home and Office Users." November 5, 2001. URL: http://online.securityfocus.com/infocus/1504
[ix] Siepmann, Frank. "SOHO Security Solutions." April 3, 2000. URL: http://www.networkcomputing.com/1106/1106ws2.html

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.