Global Information Assurance Certification Paper

Implementing Security in a Small Non-Profit

Roger Jacobs

Version 1.4b

This is a case study about how security has been implemented in a small non-profit organization. I have chosen this topic because the constraints on a small organization can be quite different from their larger counterparts. For example, cost is usually a larger constraint and ease of management due to a small IT department. Most of the reading materials that are currently available cater to companies that have all the resources they need in order to secure their company. This includes plenty of manpower in IT and budgets that take security into account. I hope to give some insight into the decision making process for securing small networks where security needs are equally important. The other point I hope to convey is that being small enables the IT department to give more personal explanations on why things need to change in order to improve security. This includes user instruction as well as explaining to management.

I will go over the primary areas of the organization by painting a picture of where we started. This will include the network, servers, workstations, passwords, virus protection, and finally patching. From there I will explain what changes we made and why. Finally I will point out where we succeeded and where we still come up short.

Before:

Our organization is similar to other entities that started out small and over time has grown larger. A company of 10 employees is now a company of 150 employees. We started with no computers, to perhaps a couple for necessary communications, to having file, email, and print servers. Anything that has been implemented is due to a need. An example of this would be email. The employees need email so an email server is setup using the most basic of default settings for everything. It works and that is all that matters. Computers and networks have been put in place where needed and security is not factored in at all.

The Information Technology (IT) department consists of a Director and a Network Administrator. All tasks, from desktop support to router programming, are handled by one of these two people.

I will go through each area in detail below.

Network:

We have nine offices across the country. Each office is a stand-alone network. How each network is configured could change from office to office. Every office has a broadband connection of some type. The ISP or we, depending on how it was setup, manage the router in each office. Firewalls are nonexistent. 10Mb hubs are usually the norm and these were typically low-end 3com models. Cat5

and cat3 cabling connects everything. All but one office is setup with static private IP addresses with Proxy Server 2.0 being used for NAT. The one office that is not using private IP addresses has static public IP addresses assigned to each computer. The physical location of the equipment is completely unsecured. Any employee has access as well as any guests or cleaning staff.

Servers:

All of the servers are Windows NT. Each office is its own domain with zero trust relationships setup. Each office only has one server and 90% of the time the server is just an authentication server, file server, and print server. These servers also provide name resolution services at least for domain resources via WINS. The Office Manager in each respective office handles backups on their server. Finally, the physical locations of the servers in the regional offices are the same as the networking equipment mentioned above.

The headquarters has two extra servers beyond the combined authentication, file, and print server. This would include the email/intranet server and an Oracle database server. The database server is configured to only be used inside the network. The email/intranet server uses Exchange 5.0 and IIS 5.0. The Exchange is configured for clients to connect remotely and POP their mail or connect over the Internet using Outlook Web Access (OWA). It should also be noted that this server is in the same domain as the one used for all of headquarters. All of the hardware in the headquarters is kept behind a locked door that only the IT staff has access to.

Workstations:

The workstations are a mixture of Windows 3.1 and Windows 9x with 9x holding about 95% of the desktops. Every workstation has Eudora installed (version numbers vary greatly from machine to machine) configured to POP mail from the email server.

Passwords:

Users are assigned a noncomplex password that is generated by the administrator. Every password follows the same scheme. An example of a password would be 'house853'. The first part of the password is a word that is assigned to the department. Therefore all the people in the Marketing department would have the same word in the beginning of their password. The last part of the password was always three numbers randomly pressed by the administrator when they created the account. These passwords never expire and cannot be changed by the user. All the passwords are kept in an Excel file that is password protected with another noncomplex password.

The reason that these policies for passwords exist is because the IT department does not know how to allow the user to change their password on their domain and on the email server at the same time. If a user were allowed to change their password, their network credentials and their email credentials would be different. If the passwords on the email server were set to expire, the user would have no way to connect to that domain and change their password.

Virus Protection:

Most workstations have Norton Antivirus installed. The version differs on each computer merely because the installation was done haphazardly. Each configuration is completely different as well. The ability for the application to download new virus definitions is unknown. Some of the installs are still allowed however some have reached the end of the one-year free updates.

The servers do not have any virus software installed.

Patching:

Throughout each fiscal year, an office will get one visit by someone in the IT department. During that visit the IT professional would update the servers and workstations with new service packs, hotfixes, and patches. If any new updates come out between the visits, even critical updates, they are not applied until the office visit.

During:

Now that we have a decent picture of where we started, we need to figure out what we are going to do. A decision is made to increase the size of the IT department and bring in someone to split their time between database management and everything else. Everything else would entail desktop support, network administration, security, and server management.

Understanding the idea of defense in depth, we know that we want to improve the security across all fronts. Every piece of our infrastructure that I listed above should be made more secure after we are finished. The idea here is that we may not have the best firewall on the market, we may not have every single hotfix for the operating system, perhaps our antivirus software is not configured for maximum secure operation, but with all of these pieces added together, we have defense in depth and we are able to protect our information.

Network:

Most early decisions are made based on best practices. Articles in all major publications pretty much spell out that you have to have a firewall on your network or you are not doing due diligence. The first rule for system administrators from Lincoln Stein's book Web Security: A Step-by-Step Guide is "use a firewall to protect the internal network."[1]

The first change we make starts with firewalls. It is obvious that we need to block access to our network from the outside. This is easy to explain to management and approval is not difficult.

The firewalls we choose based on cost parameters as well as business needs. The regional offices want the ability to collaborate with each other and the IT department wants to allow users to change their passwords on the email server. We know that the best way to accomplish this is with the use of a VPN. A VPN would allow our offices to communicate securely with one another via encrypted tunnels. After much research we decide to go with SonicWALL's hardware. They make some of the more inexpensive models on the market, which meet our cost requirements. The particular models we choose come with VPN technology built in. We buy SOHO/50's for the regional offices and a larger Pro 200 for the headquarters.

We set up all the firewalls to block all incoming traffic at every office except the headquarters where we need to allow email and web traffic. This is relatively easy to do as all SonicWALL products come with an easy to use GUI. The VPN's are originally setup using strong encryption. This means using ESP in the header and 3DES for encryption. We quickly find out the reason that the SonicWALLs were inexpensive. We experience extreme lag between the offices with these settings. The hardware just can't handle that level of encryption and keep things moving smoothly. We decide on a lower encryption, ArcFour, and kept ESP.

At this point the firewalls take over NAT and we decide we no longer need the Proxy Service. There is no real security decision behind this. It just makes sense to eliminate something that appears redundant.

We give management of the routers to the ISP wherever we can based on a business perspective and not a security one. There is no one in our organization that understands routers well enough to know if they are properly configured. The amount of money to either train or hire someone for this job compared to the benefit we reap from it makes the decision very easy. We make the assumption that the ISP has people that are competent and that if anything were to go wrong, they would be responsible.

[1] Stein, Lincoln. Web Security: A Step-by-Step Guide. Addison-Wesley Longman, 1998.

Where possible we try to reduce physical access of routers, firewalls, and hubs. The solution for most offices is moving the equipment to a closet. This at least reduces the access that employees or guests may have.

Servers:

It is important to get all of the servers off of Windows NT and onto 2000. The largest driving force for this is Active Directory. We want to use it "for all credential management, for security and authentication. This means that we no longer have a single point of failure, like a primary domain controller in the past."[2]

Over a two-year process we upgrade all servers to Windows 2000 Server. This decision was extremely easy. Not only is it a much more secure platform, but it also gives us a lot more control over security through the use of Active Directory and Group Policy. With both of those tools we can quickly and easily setup and manage all of our users' privileges and permission access levels.

There was no special way for us to quickly update all of the servers so when we make an office visit to install the new firewall and VPN, we also install Windows 2000 Server. We do our best to harden the servers by making sure that only the services we need are running and by not installing superfluous applications.

Using the VPN to setup one WAN for all of our offices we decide to go with a one domain model. Thanks to Active Directory we can setup Organizational Units where we can specify security policies on a more granular scale.

The email server is upgraded to Exchange 2000. One of the major decisions we make is to follow one of Microsoft's whitepapers on setting up a secure Exchange server with OWA access. In this setup you have a front-end server and a back-end server. "Because the front-end server has no user information stored on it, it provides an additional layer of security for the organization. In addition, you can configure the front-end server to authenticate requests before proxying them, protecting the back-end servers from denial-of-service attacks."[3]

Workstations:

Windows 98 and 3.1 are known to have no file protection on the local machine. We consider these operating systems to be completely unacceptable for our new vision of the network.

---

[2] Christenbury, Ben. "Microsoft Support WebCasts: Microsoft Windows 2000: Directory Services, Part One". January 13, 2000. Microsoft Corporation. http://support.microsoft.com/servicedesks/webcasts/wc011300/WCT011300.asp.

[3] "Microsoft Exchange Server: Microsoft Exchange 2000 Server Front-End and Back-End Topology". July 2002. Microsoft Corporation. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/maintain/optimize/e2kfront.asp.

Over the same two years that we replace all the NT servers, we also replace all the Windows 98 and 3.1 machines. Here is another upgrade we make when doing an office visit. When we are finished, there are only Windows 2000 Professional workstations on our network. This gives us the protection of forcing a user to have logon credentials in order to even get to a desktop.

We also use Group Policy to enforce a secure template on all the workstations. We use "compatws" security template that allows the users to run legacy applications without giving them elevated rights. Before we were using Group Policy we were forced to make users Power Users so that they could run some of the software they needed.

This change requires training at each office. Here is a great example of where having smaller groups to deal with makes life easier. The training sessions always involve extensive Q&A at the end. We use this information to improve upon the next set of training and to improve the way that we implement the changes.

Passwords:

Passwords are the number one place that we need serious change in. Everything that we are doing created an environment for zero responsibility or accountability. The company culture has become one where passwords are shared with anyone because someone in the IT department already knew the password. The attitude is: "What dose it matter if the person I work with knows it as well?"

It is extremely important that the directive for any change comes straight from the head of the organization because people are used to the way things are. I'll explain below how we get higher management to buy in.

Now that we have a WAN setup through the VPNs we can allow our users to easily change their password and not only will their local server be updated, but the email server as well. With this new ability we decide it is time that our users start to come up with their own passwords. We use Active Directory to force complexity, three out of the four requirements (lowercase, uppercase, number, and symbol), length of eight, 90-day expiration, and they can't use the last five previous passwords.

Here more then any other changes we make, we need to convince management that this is a good idea. We explain to them the idea of sensitive information and how we don't want just anyone to have access to it. In other words, the confidentiality of our information. We give an example of how someone can send email on behalf of another user and ruin the integrity of our organization. Finally, we offer examples of angry employees deleting entire documents so that the information is no longer available.

Management eventually agrees that the password policy is a good idea, which means that all the users were forced to go along as well. Without management we had several people complaining that the whole process was just a waste of time. People argued that 90 days was too short of a time period, which would force people to write their password down. Other complaints included the complexity and length requirement being too difficult. However, I can report that after the policy was in place, everyone dealt with it just fine.

Virus Protection:

Since malicious code can hurt the integrity, confidentiality, and/or availability of information on our network, virus protection definitely falls under security. We knew this first hand because a few viruses had hit us due to the lackadaisical approach that was taken in the past. The amount of time and effort that was spent on cleaning up those accidents could have been avoided if we were more vigilant.

Since we already had Symantec products installed on all of our workstations, we decided to just upgrade the software. However, we know that we need a better way to manage all the individual clients. Thankfully Symantec created Symantec System Center (SSC). With SSC we can manage every single installation of AntiVirus that we have.

We install SSC on each main server in all the offices and make a group for every location. From there we install the clients that then look to that same server for updates. This includes software updates, virus definitions, and any configuration changes. Now every client has virus protection and it is locked so that they cannot tamper with it. The clients look to the primary server in their group every 60 minutes for new definition files. Realtime virus protection is running at all times on the client machines

The servers also get virus protection installed to each of them. Again, realtime virus protection is always running. We have to make sure to exclude particular folders on the database servers and the Exchange server. Once every week the entire server is scanned for anything that the realtime virus protection might have missed.

Norton AntiVirus for Exchange is installed on the email server. This allows us to catch any virus that comes through email.

Patching:

Patching is another way to protect against viruses. A report by the CERT Coordination Centre at Carnegie Mellon estimates that more than 95 percent “of intrusions result from exploitation of known vulnerabilities or configuration errors

where countermeasures were available."[4] Many of the countermeasures CERT is referring to are patches.

Every time that we upgrade a workstation or server to Windows 2000 we update it with the latest patches. The first process is to go to windowsupdate.microsoft.com. All critical updates are applied and a few of the recommended updates as well. After that we use the Microsoft Baseline Security Analyzer (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp) to scan the computers for any other patches that we may be missing.

Keeping up on critical updates currently falls on the Office Managers. This is not the ideal solution because they do not consider any IT work to be their primary job function. We are interested in improving on this process and make things more automatic without requiring the Office Managers involvement.

After:

Is the organization more secure than the "before" picture? Yes. We have done our best to cut out as much vulnerability as possible. We have followed the defense in depth method and not relied on anyone one technology to protect us from every threat out there. We have learned that being a nonprofit doesn't mean that you cannot be secure. Most companies that we purchase from give discounts to nonprofits which helps with the cost restrictions. Finally, we have learned that security has to be a company wide involvement and this is where being smaller pays off. We have the ability to give lessons and instructions to each office on a rather small scale. We can take individual questions and help people to understand why certain practices are important. If the entire company did not go along with the process, we would have failed. Users could have decided to write their password down and keep it under their keyboard. Management could have decided that virus protection was a waste of money sense they never see the repercussions. Through education and extensive reporting, we were able to secure our entire organization.

The following are examples where we still need to improve.

For all intents and purposes we have ignored the insider threat and only focused on the people trying to get in. This is the way most people work in our organization. Complete trust of the people you work with. The IT department would like to still close down more vulnerabilities from the insider threat. If someone unwittingly unleashed a virus on our network, the amount of damage

[4] "CERT/CC Overview: Incident and Vulnerability Trends". March 4, 2002. CERT Coordination Center. 1998-2001 by Carnegie Mellon University. 16. http://www.cert.org/present/cert-overview-trends/module-2.pdf.

that can be done would be greatly reduced if that user's abilities on the network were also greatly reduced. This will require more attention to Active Directory and Group Policy.

The backups are still being handled by the Office Managers. This situation is not ideal because the backups need to run regardless of illness, vacation, or memory lapse. Therefore, backups do not always happen on a consistent basis. We are in the process of creating a centralized backup located at the headquarters. The impediment we need to solve there is replicating the data for all 9 offices over the VPN. Hopefully we will solve that one soon.

The VPN protection could be increased. SonicWALL has released products that are more robust then the early models we purchased. We hope to switch over to these models and take advantage of 3DES encryption for our entire network.

We are working on a server to push out hotfixes and patches so we can increase how quickly critical updates can be applied. We are in the process of testing a Remote Update Server, however there are a few questions we still need answered: Should we apply patches to a test network? If so what procedure should we follow to make sure everything still works? What tools do we need to verify that the patch fixed what it was suppose to?

Physical security is something that we definitely don't pay enough attention to. Something that we are painfully aware of is that "if your computers are physically compromised, stolen, or destroyed, it is very difficult to protect your data or ensure its availability."[5] Our ability to physically secure equipment varies from office to office and we hope to address this issue in greater detail in the future. Perhaps cages for the equipment that can only be accessed by an IT employee.

[5] Shawgo, Jeff. Securing Windows 2000. Version 1.5, July 1, 2001. The SANS Institute, 2001. 15.

References:

1. Stein, Lincoln. Web Security: A Step-by-Step Guide. Addison-Wesley Longman, 1998.

2. Christenbury, Ben. “Microsoft Support WebCasts: Microsoft Windows 2000: Directory Services, Part One”. January 13, 2000. Microsoft Corporation. http://support.microsoft.com/servicedesks/webcasts/wc011300/WCT011300.asp.

3. “Microsoft Exchange Server: Microsoft Exchange 2000 Server Front-End and Back-End Topology”. July 2002. Microsoft Corporation. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/maintain/optimize/e2kfront.asp.

4. “CERT/CC Overview: Incident and Vulnerability Trends”. March 4, 2002. CERT Coordination Center. 1998-2001 by Carnegie Mellon University. 16. http://www.cert.org/present/cert-overview-trends/module-2.pdf.

5. Shawgo, Jeff. Securing Windows 2000. Version 1.5, July 1, 2001. The SANS Institute, 2001. 15.