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.

Information Security For Churches and Small Non-Profit Organizations

In today's ever changing, better, faster, cheaper world, connectivity to the Internet for churches and other small non-profit organizations is necessary. But, connectivity brings along with it a risk of vulnerability from the same threats that business and educational organizations face. Hackers and other harm-doers will not make an exception for these low budgeted and resource strapped organizations, and if an opportunity is found that can be exploited, you can bet someone, somewhere will exploit it. The potential rep...

Copyright SANS Institute

Author Retains Full Rights

AD

Information Security
For Churches and Small Non-Profit Organizations
(Security On A Budget)

GSEC Practical Assignment
Version (1.4b) Option 1

Jay C. Petel
April 8, 2004

© SANS Institute 2004, Author retains full rights.

Table of Contents

Table of Contents....2
1. Abstract....3
2. Introduction....3
3. First Things First – Start With the Basics....5
   3.1. Technical Help....5
   3.2. Backups....6
   3.3. Policies, Standards and Guidelines....6
   3.4. Physical Security....7
4. Securing Your PC....8
   4.1. Locking Down Your PC....8
   4.2. Patch Management....9
   4.3. Anti-Virus Software....10
   4.4. Spy-Ware....12
   4.5. Content Filtering Software....13
   4.6. Email Spam Filters....14
5. Wireless Security....15
6. Using a Firewall....16
7. Summary....17
Appendix A - Sample Documents....19
   a. Sample Nondisclosure Agreement....19
   b. Sample Acceptable Use Policy....19
Appendix B – Diagrams....19
   a. Perimeter Firewalls....19
Appendix C – Technical Information....19
   a. Windows XP Security Settings....19
   1. Microsoft Recommended for Windows XP Home....19
   2. WindowsSecurity.com....20
   3. Double check your browser security settings....20
References....21

© SANS Institute 2004, Author retains full rights.

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

1. Abstract

In today's ever changing, better, faster, cheaper world, connectivity to the Internet for churches and other small non-profit organizations is necessary. But, connectivity brings along with it a risk of vulnerability from the same threats that business and educational organizations face. Hackers and other harm-doers will not make an exception for these low budgeted and resource strapped organizations, and if an opportunity is found that can be exploited, you can bet someone, somewhere will exploit it. The potential reputation damage along with any physical damage that occurs can have a permanent impact on the hacked organization. If contributors are using credit cards to make donations and their card numbers are compromised, think of the potential loss of income that may never be recovered over the course of time. If personal information is accessed due to a lack of security measures, the harm to both organization and member may not be measurable in dollars; however, the emotional injury and loss of credibility may be catastrophic. Also, consider a hacker taking control of machines to deliver a distributed denial of service attack on another web site. Not only are these scenarios a possibility, but these things do happen, almost every day.[1]

In order to help to prevent these things from happening to your network, several things need to be considered and acted upon when connecting your small office to the Internet. Cost has always been a primary factor for churches and small non-profit organizations. It is difficult enough to get the money to fund the reason for your organization's existence, let alone spend some of that money protecting your computers from hackers and viruses. Fear not, it is possible to implement a secure defense without breaking the bank. Not all security improvements require spending much of your hard fought for money. By taking some "free" procedural steps and also by utilizing free or low cost software you can build a reasonable security defense for your organization.

2. Introduction

Take a look around the typical office of a church or small non-profit organization and you will find a mixture of inexpensive and donated items. The office may be located in an older building which doesn't lend itself to rewiring for computers, if rewiring could even be afforded.

Volunteers also make up a large portion of the work force, which usually does not include a technologist who is capable of keeping all of the computers running securely. Maybe you have a member/volunteer or some other in-house helper who thinks of themselves as a computer expert but, in fact, has very little relevant experience and cannot provide the type of

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

detailed expertise that you require. Perhaps your technologist may have been the store clerk at the local electronics or office supply store where you bought your computer. On his or her recommendation, you built a network with $500 computers and a low-cost wireless router. Now you are on your way to the computer super-highway!

But wait, didn't you hear that there are devious people out there trying to do damage to your computer? What are you going to do about it? Where should you begin? According to the *SANS Institute list of The Five Worst Security Mistakes End Users Make*[2], users leave themselves vulnerable by:

1. *Failing to install anti-virus, keep its signatures up to date, and apply it to all files.*
2. *Opening unsolicited e-mail attachments without verifying their source and checking their content first, or executing games or screen savers or other programs from untrusted sources.*
3. *Failing to install security patches-especially for Microsoft Office, Microsoft Internet Explorer, and Netscape.*
4. *Not making and testing backups.*
5. *Using a modem while connected through a local area network.*

Sans also identifies *"Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job."* as the number one worst mistake that senior executives make.

First things first, let's take a close look at exactly what a security defense in depth really is, then we can figure out how to implement it.

Let's begin with finding some help. Perhaps you are lucky enough to have an IT professional available to do the work for you. If not, then you need to search for the right person. You will also need to establish a sense of trust and confidentiality with them. Next, be sure you are backing up valuable data stored on your computers. Can you easily recreate anything that you lose if one of the computers broke or was stolen? Also, developing acceptable use and other policies will help by defining what right and wrong is. Once you have established right and wrong, you can then build your security defense to assist with keeping things from getting out of hand.

Specific security steps on your computer are necessary to implement. Right out of the box your computer is a friend to hackers, not to a secure computing environment. You will need to protect yourself from viruses. Can you be sure the anti-virus software included with your pc is active and protecting you? Are you being monitored by spy-ware that, unknowingly to you, has been downloaded on to your computer? How about spam filters for your email? Aren't you tired of sorting through all of that unnecessary junk email? Do you need to implement some form of Web content filtering? Are

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

there children around or other adults that would be offended by accidentally seeing pornography pop up when they really meant to visit www.whitehouse.gov but instead went to www.whitehouse.com?

Locking down access to your wireless router is imperative. The frequency of WAR driving, i.e. people driving around looking for unsecured wireless connections, is increasing. For example, according to the Detroit Free Press, "*Two young men sitting in a car in the parking lot of a Lowe's home improvement store in Southfield repeatedly hacked into the company's national computer network over the past two weeks, gaining access to credit card numbers and other information, federal prosecutors said Monday."* [3] Nor do you want someone sitting in your parking lot using your network to hack into someone else's network.

By building a comprehensive defense in depth security plan utilizing free and low-cost solutions, the networks and computers in the offices of churches and small non-profits can be protected without "breaking the bank."

3. First Things First – Start With the Basics

3.1. Technical Help

First of all, if you feel you are not confident that your computer knowledge is sufficient you must get some technical help. It may not be easy, but finding someone with technical expertise who can become familiar with your environment will help with development and implementation of a systematic security plan.

Finding technical help is in many ways similar to finding a car mechanic you can trust. If you are lucky, you may have the skill, time and desire to do some of the maintenance work on your car, and as a result you do not need to have a regular mechanic. But, if you are like most people, your time is better spent on other things. Either you have found a reliable mechanic that you trust or you go from mechanic to mechanic hoping to be treated fairly and not be taken advantage of. Think of technical computer help this way. Find someone you can trust and who is reliable and you will be well on your way to keeping your computers up and running securely.

Be careful of your own in-house computer expert. It is very unlikely that you have someone available to you as a member or volunteer who really has the type of experience that you require. Find someone trained in security techniques; don't make the mistake to use a non-professional. As SANS warns, it's a mistake *"allowing untrained, uncertified people to take responsibility for securing important systems."* [4]

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

Word of mouth, looking to local user groups, or searching for volunteer technical organizations on the Internet can be a quick way to find someone with the right level of expertise. If finding someone this way does not work, check with local integrators, who may have a pro bono policy for their technical staff.

After finding someone to help out, be sure to have them sign a nondisclosure agreement. As TechRepublic puts it: *"When contractors, consultants, or third-party vendors work in your organization, your proprietary information is vulnerable. Protecting this sensitive enterprise information should be a top priority. Signing a nondisclosure agreement (NDA) between you and an external party can help."* [5] You can download nondisclosure samples from the TechRepublic web site and modify them to fit your needs. Remember it is a good idea to seek legal counsel before you create and sign an NDA with an external party.

3.2. Backups

Once you are on your way to getting some tech help, move on to taking care of a few basic but valuable items. Backups. As much of a nuisance it is to make regular backups, the need to rely on them just once is more than worth the effort.

Your main reason for backing up your computer is to have an insurance copy in case of a disaster. For example, system failure could cause a loss of all of the information and programs on your hard drive. You might work in an area that is prone to natural weather related disasters like hurricanes or tornados. Regulations and audit requirements may dictate saving backups in an offsite location with very specific rules regarding how long to save them.

Determining whether to backup only your data or have a complete backup of your computer is solely based on how long it takes to restore all of your programs from the original CDROM's, (if you can find them.) Perhaps a combination of both complete backups and data only backups is your best option. This way you will have the security of knowing you can completely recover your pc from a backup or quickly grab a document that needs to be recovered without traversing through a complete backup.

3.3. Policies, Standards and Guidelines

Another of your fundamental steps to a security defense in depth plan is to develop and implement policies that define appropriate behaviors and actions covering many different areas. In addition, standards and guidelines should be documented in order to assist your policies by defining the details

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

referenced by the policies. Protecting business and personnel data, acceptable use of office computers, emergency procedures, and anti-virus protection are among the many topics you can document, the trick will be to implement something that will be both valuable and enforceable.

According to an article in the November 2003 edition of CSO magazine, there are four parts to developing policies.[6]

- *Identifying and communicating risk – What's the problem?*
- *Creating an accepted policy and guidance infrastructure – What do we expect accountable parties to do?*
- *Developing processes to monitor conformance with policy – How do we know we are successful?*
- *Preparing, when the controls fail, response capabilities – If it hits the fan, who will do what to mitigate it?*

Enforcement and auditing of the policies can be tricky, but very important when it comes to keeping your policies alive and in place. If no one cares about the policy, why then should anyone follow it? Before implementing your policies, it's best to launch an education and awareness program. [7] Promoting awareness among all employees will help make security everyone's job.

Standards will be the bulk of the documentation you will create. These will define exactly how particular measures are accomplished. You may have a standard that no personal software is to be loaded or not to share passwords.

Guidelines are either a recommendation how to do something or what might be considered the best practice for your office. These procedures will address the "why we do what we do" questions that people have regarding security practices. Locking desks and cabinets guidelines will explain why it is important and how it should be properly done. By having guidelines, everyone in the office will be able to have the confidence they are following the correct and same procedures.

To find sample policies, standards and guidelines on the web, visit the SANS web site at http://www.sans.org/resources/policies.

3.4. Physical Security

Take care not to ignore physical security. Maybe you can't lock your door during business hours, but you can take precautions to keep unauthorized people away from your assets. Whether it's preventing theft of equipment or people dumpster diving for sensitive information, consider physical security your number one priority. Shred old documents with sensitive information and

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

make sure employees have a place in their work area that can lock for storing sensitive information. Look around your office and implement simple but effective physical security processes and policies that will help reduce the risk of loss of sensitive data and equipment.

4. Securing Your PC

4.1. Locking Down Your PC

To quote the web site UK Security Online Limited, "*Out of the box Windows XP is as insecure as all of Microsoft's attempts at operating systems. All their (Microsoft's) efforts go towards making Windows XP easy to use and very little towards the security consideration since this makes for a less comfortable operating environment. However, the world has changed significantly and more effort must be made if your PC is not going to share your personal information with anyone in the world who cares to look."* [8]

But, if you apply the suggested security guidelines it will make your pc a little harder to hack into. That's right, harder, not impossible. No computer is impossible to hack once you connect it to the Internet. Your computer is still vulnerable in some way and your best defense is to make their work a little harder so that they will move on to some other potential victim. By enabling the NTFS file system, encrypting folders, enabling ICF (the built-in firewall), limiting the number of administrative accounts, ensuring all accounts require strong passwords and disabling unnecessary services, you will greatly improve your system's security.

In addition to the UK Security Online web site, you can find both XP Home and Professional checklists on the Microsoft TechNet web site at the Windows XP Baseline Security Checklists page, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/xpcl.asp. You can also find more security setting guidelines on the National Institute of Standards and Technology web site and by downloading the document SECURE CONFIGURATION OF WINDOWS XP PROFESSIONAL SECURITY TECHNICAL IMPLEMENTATION GUIDE, http://csrc.nist.gov/pcig/STIGs/WindowsXP.doc.

As a first step, download and run the free Microsoft Security Baseline Analyzer from Microsoft's TechNet web site at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp.

When you run the analyzer, your system will be reviewed for common security misconfigurations. The results are presented back to you with the worst vulnerabilities shown first.

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

Keep in mind that the items highlighted by Microsoft are only a "baseline". There are many more items that go well beyond what Microsoft recommends which will take your system to a more secure state. The Security Baseline Analyzer also provides you the benefit of checking your patch status.

4.2. Patch Management

According to the CERT® Coordination Center, since early 2002, there has been an average of 11 security vulnerabilities reported every day.[9] In response, you will find that Microsoft attempts to address these vulnerabilities and provides updates to their Windows operating systems on a regular basis. These updates are extremely important to apply in order to keep your system from being susceptible to attack. As stated by Gregory Toto in a whitepaper from BigFix, Inc.[10], *"A first line of defense is to patch security holes, thereby closing the door on the most common entry point for security threats in a network."* He also goes on to say:

> *Computer vulnerabilities are extremely costly to American businesses and government organizations. According to IDC, enterprises and government agencies will spend upwards of $20 billion in 2003 on the problem of Internet security vulnerabilities and, according to Gartner, another $11 billion on systems management solutions. The costs that result when organizations leave issues unresolved or undetected, and must react to security*

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

incidents, such as the recent Nimda, Code Red or SQL Slammer attacks, push these numbers even higher.

There are several options available to automatically keep your systems up-to-date with the latest patches. You can follow Microsoft's online process for configuring the built-in firewall and automatic updates. http://www.microsoft.com/security/protect/windowsxp/choose.asp Using Microsoft's automatic update feature, you can specify how you want Windows to update your computer. Once you configure this option, you will begin receiving notifications whenever it finds updates available for your computer.

You can also look to third-party vendors such as BigFix for a free consumer version of their patch management software from http://help.bigfix.com. These third-party products will typically scan your computer for more software than just Microsoft's and alert you to updates as they become available.

Also, by keeping systems up-to-date with the latest patches, you will find a side benefit of a better running computer. Frequently, the problems that are patched not only close a security hole, but will also keep your systems running more stable.

Keeping your systems patched will help to prevent viruses, worms, and Trojan horses like the Slammer or CodeRed from infecting your system. The vulnerability which Slammer took advantage of had a patch issued from Microsoft nearly six months before Slammer was released. Do your part to prevent the spreading of these viruses, worms, and Trojan horses, keep your systems up-to-date with patches!

4.3. Anti-Virus Software

Patching is part of a one-two punch to avoid viruses, worms, and Trojan horses. The other way to keep your computer safe once you have connected it to the Internet is to install anti-virus protection software and keep it updated.

According to F-Secure, the first anti-virus web site, there is now a total of over 90,000 known viruses in existence and *"The year 2003 has clearly been the worst in history."*[11] But what type of problems do viruses cause and what are the real issues with them? F-Secure explains:

> *The network congestion caused by Slammer dramatically slowed down the network traffic of the entire Internet. One of the world's largest automatic teller machine networks crashed and remained inoperative over the whole weekend. Many international airports*

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

reported that their air control systems slowed down. Emergency phone systems were reported to have problems in different parts of the USA. The virus even managed to enter the internal network of the Davis-Besse nuclear power plant in Ohio, taking down the computer monitoring the state of the nuclear reactor.
The RPC traffic created by Blaster caused big problems worldwide. Problems were reported in banking systems and in the networks or large system integrators. Also, several airlines reported problems in their systems caused by Blaster and Welchi, and flights had to be canceled. Welchi also infected Windows XP-based automatic teller machines made by Diebold, which hampered monetary transactions. The operation of the US State Department's visa system suffered. The rail company CSX reported that the virus had interfered with the train signaling systems stopping all passenger and freight traffic. As a result of this, all commuter trains around the US capital stopped on their tracks.

Although according to CSX, the trains were halted voluntarily due to the slowdown of dispatching and signal systems. [12]

Keeping your virus definitions up-to-date is extremely important. Too often people don't configure their anti-virus software to download the latest virus definitions. This is like getting a flu vaccination once and never following up with additional shots in following years. You may be temporarily protected, but some new virus will come along that your vaccination does not protect against. Anti-virus software is much like this, it is not enough just to install it, the true value is to keep getting the updates to the virus definitions on a regular basis. Check out the Top Ten Viruses Reported to Sophos In November 2003[13] and you will see that five of the top ten are less than a month old and the remaining five are no more than six months old.

Many of the computers that you can buy today have anti-virus software installed, and all you need to do is purchase the annual subscription for the virus definition updates. You can also find free software with free virus definitions from Grisoft at http://www.grisoft.com/us/us_index.php.

Beyond keeping your anti-virus software updated, you should follow these tips from F-Secure:[14]

- *Configure Windows to always show file extensions. This makes it more difficult to for a harmful file (such as an EXE or VBS) to masquerade as a harmless file (such as TXT or JPG).*
- *Never open e-mail attachments with the file extensions VBS, SHS or PIF. These extensions are almost never used in normal attachments but they are frequently used by viruses and worms.*
- *Never open attachments with double file extensions such as NAME.BMP.EXE or NAME.TXT.VBS*

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

- *When you receive e-mail advertisements or other unsolicited e-mail, do not open attachments in them or follow web links quoted in them.*
- *Avoid attachments with sexual filenames. E-mail worms often use attachments with names like PORNO.EXE or PAMELA_NUDE.VBS to lure users into executing them.*
- *Do not trust the icons of attachment file. Worms often send executable files which have an icon resembling icons of picture, text or archive files - to fool the user.*

By using anti-virus software and following these tips, you will help to prevent your systems from getting infected with a virus, worm or Trojan horse.

4.4. Spy-Ware

Today many companies have built a business model on collecting information about your web browsing habits and then selling that information to other companies in order to target advertising to your specific interests. To accomplish this, these companies secretly download software to your computer and, unknowingly to you, report back to them your activities. Steve Gibson, founder of Gibson Research, defines Spyware as any software that employs a user's Internet connection in the background without their knowledge or explicit permission.[15] These spy-ware programs are not only a violation of your privacy, but they also affect the performance of your system and consume Internet bandwidth.

The Center for Democracy & Technology wants Internet users to detail their unpleasant experiences with spyware. They hope to compile these experiences and submit them to the Federal Trade Commission in the hopes the FTC will take action against businesses that do not clearly inform users about the presence and potential actions of spyware. The CDT challenges that "*Computer users are increasingly finding programs on their computers that they did not know were installed and that they cannot uninstall, that create privacy problems and open security holes, that can hurt the performance and stability of their systems, and that can lead them to mistakenly believe that these problems are the fault of another application or their Internet provider.*"[16]

To find software to seek out the spyware on your systems and remove it, you can visit http://www.spychecker.com/ where you will find the top 25 downloads that will help you with privacy and spying issues on your computer. A product called Ad-aware is available from Lavasoft (www.lavasoftusa.com). You can download the free version of Ad-aware from several sites that are listed on Lavasoft's web site. Many people find

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

their systems run much better after removing the spyware that was installed on their computer.

4.5. Content Filtering Software

Have you ever mistyped a url and found yourself transported off to an adult web site? It is easy, you might not even realize what you typed and there you are, stuck in a web site full of pop-up windows and it just won't stop. It could be very embarrassing for you and it could also cause a problem if someone is offended by what they see on your screen. The website www.whitehouse.com is probably the most famous of these, getting press coverage by ABC News, CNN, MSNBC and Newsweek.

But peddlers of pornography are not the only opportunistic people out there. "Typosquatters" register hundreds of domains eager to take advantage of keyboard-challenged web surfers. They make money by redirecting you to another site which pays them a fee for each surfer they redirect or by opening up banner ads when you arrive at their misspelled web site.

Employee use of the Internet for non-business related activities is significant and can put a strain on your valuable Internet bandwidth. With more and more companies restricting access to the Internet for non-business reasons, it is likely you will need to consider doing this too. Controlling employee's access to the Internet is not only a productivity concern for employers, but a legal liability too. In an article by TechRepublic, Managing Content Security:Update 2002[17], indicating that corporate liability needs to be taken into consideration, they state: *"Another serious risk for inappropriate or unauthorized use of enterprise Internet or e-mail resources is the liability that may accompany such use. Even those organizations with Acceptable Use Policies (AUP) are exposed to risks from legal or other serious ramifications when their employees abuse enterprise resources. When employees do engage in unapproved activities, the survey data demonstrate that many organizations dismiss the violator. In fact, 53 percent of respondent organizations have fired employees for inappropriate use of enterprise Internet and/or e-mail resources."*

How can you control this problem without having to improve your typing skills or running around watching your employees' use of the Internet? Try using web content filtering software. Popular pay-for software such as SurfControl and WebSense are available that not only block web content but also integrate into email and instant messaging to assist with spam and unauthorized use of instant messaging. Unfortunately, these two products may be more expensive and complex than you may be able to afford and support, so look to other products such as CyberPatrol at $39.00 per year. A free content filter is available from We-Blocker (www.we-blocker.com),

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

but offers only limited control over the filtering. Most of these products will log activity, so that you can review people's Internet activity if necessary.

4.6. Email Spam Filters

"Spam is no longer just a nuisance: It is quickly becoming both a potential legal liability and a major productivity drain on corporate IT departments and corporate users alike. More than 40% of the respondents to IDC's email retention survey (which recently surveyed 557 North American organizations) indicated that the number of spam emails received during an average day has risen (by) 50. 100%, compared with the number received 12 months earlier." [18] If you have an email account, I'm sure you probably agree with this statement from IDC. Your in-box contains more junk email every day and it's only getting worse.

What can you do to stop it? Pretty much nothing will stop it, but you can reduce what you have to deal with. If you use AOL, MSN or Yahoo mail, they have their own spam filters built in. But, if you use Microsoft Outlook, there are a couple of options for you to try. It's going to take some work, but in the end it will be worth it.

First, there are some guidelines to follow that will reduce the amount of junk email you receive by following these recommendations from Microsoft.[19]

- *Avoid replying to the sender trying to remove you from their mailing list. Many senders use this to confirm that they've reached a working email address.*
- *Alter your email address when posting. Some organizations scan web pages and newsgroups to harvest email addresses. Alter your address in such a way as to trick search programs but not confuse users.*
- *Avoid giving out your primary email address. Guard your main email address just as you would your telephone number. Set up a second email account to use for filling out forms and sign-up offers on the Internet.*
- *Set up rules to move junk mail and adult content messages to a special folder. Outlook has built-in filters and you can create your own custom filters to deal with junk email.*

In addition to the built in rules in Outlook, there are several free tools you can use. SpamBayes (http://spambayes.sourceforge.net) a free tool, is a plug-in to Outlook that will learn what you consider spam and then automatically move new messages into a special folder. You will need to teach SpamBayes what junk mail is, but then it will compare that knowledge against new mail and automatically classify your mail into two categories;

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

spam and good mail. Another good product SpamPal (www.spampal.org) is also free.

When you control the amount of spam that your employees have to deal with, you will realize added productivity. Recently, in a Secure Enterprise Magazine article, Houston based M.D. Anderson Cancer Center at the University of Texas calculated that it costs $1 for each unwanted mail message that gets through to user's computers.[20] The article goes on to quote a Nucleus Research study that spam costs U.S. companies $874 per employee per year in lost productivity.

5. Wireless Security

Wireless security may be the most significant precaution you can implement, because without some level of protection on your wireless access point, you are basically wide open to attack. With costs quickly coming down and technology rapidly improving, you can build yourself a cost efficient and powerful wireless network, but, the slightest misconfiguration can lead to a gaping hole in your in depth security plan. Even while traveling, you need to be aware that the wireless adapter in your laptop may allow someone else with a wireless adapter to connect to your laptop without you knowing it. Keeping all of the security in depth pieces in place and up-to-date is very important. But is it worth the risk to use wireless? Or should you continue using the old tried and true copper wires to connect your network together?

Just as with everything else, you can increase the level of security by applying a few simple techniques. While WEP (wired equivalent privacy), which encrypts data in either 40 or 128 bit keys, was intended to be prevent hackers from snooping your wireless network, there have been multiple automated tools developed that will break the code in a relative short period of time. The idea with much of the wireless security is to make your network less desirable to attack, not impossible to attack. Unless you're a highly visible target, a hacker will move on to attack another network that is not as well protected. Enable WEP in 128 bit mode to provide the maximum encryption.

Additional basic wireless security measures involve changing the default settings on you access point. Most vendors have a default SSID (Service Set Identifier) that you should change. Linksys uses "linksys" as the SSID on their devices. Not changing these makes it easier for an unauthorized user to gain access. Also, when you change the SSID, make it something that is not easily identifiable with your business or otherwise easily guessed. Instead, use a long meaningless string of characters that would be difficult to randomly guess. Shut off broadcasting the SSID will greatly reduce the

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

potential that your wireless access point will be discovered by someone "war driving". War driving is the process hackers use to locate wireless networks. They use a laptop computer connected to a wireless adapter attached to an antenna and simply drive or walk around looking for wireless networks to respond.

Computerworld suggests that the greatest weakness with wireless security isn't the technical shortcoming, but out-of-the-box insecure installations.[21] So by making changes to the default settings you will greatly enhance the security of your wireless access point.

6. Using a Firewall

Firewalls fall into two categories: perimeter and personal, and within these two categories, there are several firewall methodologies. Packet filter, proxy, stateful inspection and application gateways are all various ways firewalls look to control traffic. Each methodology has its strength and usually has a weakness too and many firewalls combine technologies in order to provide the best service. Most perimeter firewalls will have some form of stateful inspection and packet filtering. Perimeter firewalls are a barrier between your network and the Internet, sort of a gateway (refer to Appendix B). This is like locking the front door to your house, it's a limited amount of protection and you need to have the appropriate door to serve your purpose. Personal firewalls protect individual computers, and using the house analogy, are like locking doors to each room in your house. Remember that in a security in depth concept, firewalls alone will not protect you completely, but they are an extremely important piece of your defense. And while firewalls provide a significant amount of protection, it would be a foolish mistake to rely on them alone.

A perimeter firewall can come in several different forms. Software that is loaded on a dedicated computer, a stand-alone piece of equipment that connects to your cable/dsl modem or software built into a wireless router are all ways you can have a perimeter firewall deployed at your office. This is something you will have to purchase; quality perimeter firewalls generally do not come for free. Although there are free Linux firewalls, these are not easy to install and support unless you have solid Linux knowledge. If you are going to install a wireless network consider getting a combination wireless router/firewall. These can be found for under $150 and provide ICSA certified firewalls.

Perimeter firewalls work with a set of rules and are very detailed. On most firewalls a rule is defined by default that blocks all traffic from all IP addresses unless explicitly allowed. You then define what IP addresses are allowed into your network and also which TCP ports are allowed. You can also combine IP and TCP ports to limit specific ports from specific IP

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

addresses from sending traffic to your network. This works also to block or deny traffic from IP addresses and TCP ports. You can block all ftp traffic (port 21) from all Internet traffic. The more "allow" rules you define, the more "holes" you have in your firewall which can allow someone to break through.

Try to keep your rules to a minimum. The National Institute of Standards and Technology (NIST) says there are four guidelines for building firewalls. [22]

- *Keep it simple*
- *Use Devices as they were intended to be used*
- *Create defense in depth*
- *Pay attention to internal threats*

The more complex your design and rule base is, the more likely you will end up with configuration errors. It can be quite difficult to test each and every rule you put into the firewall, so keeping your rule base small will keep your firewall working its best as you intended it to.

Personal firewalls, in comparison to perimeter firewalls, can be found for free or little cost and there are many of them. Most personal firewalls will be a packet filter or application control firewalls. The main goal of a personal firewall will be to focus on inbound traffic coming in from the network. This includes computers internal to your network. BlackICE is a packet filtering firewall and can be configured to control outbound traffic too. This will allow you to limit people's access to other computers in your network. An application control firewall such as Zone Labs' ZoneAlarm is capable of screening incoming packets like a packet filter, but also has a rule base for applications. So if your pc tries to access another computer using an unapproved application, ZoneAlarm will stop it. This is a great protection against Trojan Horses, which try to communicate back out to the Internet without you knowing it.

7. Summary

Establishing a security in depth defense to protect your network and computers from the potential of hackers, viruses, worms, Trojan horses and other unforeseen dangers is something that is achievable without spending an incredibly large sum of money. Most of the precautions described in this paper are free and relative easy to implement, which, when implemented properly, will provide the bulk of your security defense. But don't stop there; buy what you can't get for free, your defenses are only as good as the weakest link. Spending money to keep your security tight is smart business - allowing your network to get hacked is bad business.

To summarize these guidelines for building a security in depth defense, churches or non-profit organizations should do the following:

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

1. Get your organization quality technical help
2. Backup your PC
3. Document security policies
4. Enhance physical security
5. Lock down your PC
6. Ensure your wireless access point is secure
7. Install firewalls

Once you have taken these actions, your security in depth defense is well on its way to keeping you safe and secure.

© SANS Institute 2004, Author retains full rights.

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

Appendix A - Sample Documents

a. Sample Nondisclosure Agreement

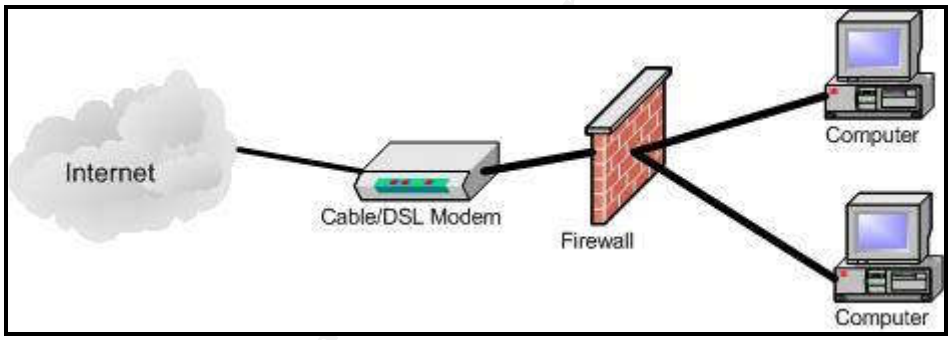
http://techrepublic.com.com/5100-6314-1038913.html

b. Sample Acceptable Use Policy

http://techrepublic.com.com/5129-6321-1635.html

Appendix B – Diagrams

a. Perimeter Firewalls



Appendix C – Technical Information

a. Windows XP Security Settings

1. Microsoft Recommended for Windows XP Home

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/xpcl.asp

- Verify that all disk partitions are formatted with NTFS
- Protect file shares
- Use Internet Connection Sharing (ICS) for shared Internet connections
- Enable Inter Connection Firewall (ICF)
- Use account passwords
- Use the Make Private feature
- Install Antivirus software and updates
- Keep up-to-date on the latest security updates

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

2. WindowsSecurity.com

http://www.windowsecurity.com/articles/Windows_XP_Your_Definitive_Lockdown_Guide.html

- Additional to the Microsoft recommendations
- Use software restriction policies
- Disable unnecessary services
- Disable or delete unnecessary accounts
- Make sure the Guest account is disables
- Set stronger password policies
- Set account lockout policy

3. Double check your browser security settings

http://browsercheck.qualys.com/

These tests automatically assess your browser for selected vulnerabilities and offer you the most up-to-date patches from Microsoft, when available.

© SANS Institute 2004, Author retains full rights.

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

References

[1] Leyden, John, "Dangerous Mimail variant knocks over anti-spam sites." The Register. Posted 03-Nov-2003. URL: http://www.theregister.co.uk/content/56/33721.html

[2] SANS Institute, "Mistakes People Make that Lead to Security Breaches", October 23, 2001, URL: http://www.sans.org/resources/mistakes.php, Copyright 2002 - 2003 The SANS Institute

[3] Ashenfelter, David. "Pair Accused Of Hacking Store System"
Detroit Free Press, November 11, 2003

[4] SANS Institute, "Mistakes People Make that Lead to Security Breaches", October 23, 2001, URL: http://www.sans.org/resources/mistakes.php, Copyright 2002 - 2003 The SANS Institute

[5] Norton, Dana, "Protect sensitive data with nondisclosure agreement"
TechRepublic, April 26, 2002, http://techrepublic.com.com/5100-6314-1038913.html

[6] Anonymous, "Policy Police," CSO Magazine November 2003(2003): 60 – 61

[7] Korosec, Chad, "Building Blocks Of Tight Security," Secure Enterprise Magazine November 2003 (2003): 58 – 59

[8] UK Security Online Limited, "Windows XP - Home User Self-Defense",
URL:http://www.uksecurityonline.com/husdg/windowsxp.php Copyright 2002 UK Security Online Limited

[9] Unknown, Cert /CC Statistics 1988-2003, October 17, 2003,
URL: http://www.cert.org/stats/cert_stats.html, 2003

[10] Toto, Gregory, "10 Steps to Automated Patch Management", October 2003,
URL: http://bbs.bigfix.com/wpreg/wpreg.htm Copyright 2003 BigFix, Inc.

[11] Hypponen, Mikko, F-Secure Corporation's Data Security Summary for 2003, December 2003
URL: http://www.f-secure.com/2003/ Copyright 2002 F-Secure Corporation

[12] Hollingsworth, Adam & Sullivan, Bob, Computer Virus Strikes CSX Transportation Computers, August 20, 2003,
URL:http://www.csx.com/index.cfm?fuseaction=company.news_detail&i=45722&news_year=2003
Copyright 2002 CSX Corporation

[13] Unknown, Top Ten Viruses Reported to Sophos in November 2003,
URL: http://www.sophos.com/virusinfo/topten/ Copyright 2004 Sophos PLC

[14] Unknown, Tips on Avoiding Computer Worms,
URL: http://www.f-secure.com/virus-info/tips.shtml Copyright 2004 F-Secure Corporation

[15] Gibson, Steve, Internet Connection Misuse & Abuse, October 6, 2003
URL: http://www.grc.com/optout.htm, Copyright 2003, Gibson Research Corporation

[16] Schwartz, Ari, Ghosts in Our Machines, November 18, 2003
URL: http://www.cdt.org/privacy/, Copyright 2001, Center for Democracy and Technology

[17] Unknown, Managing Content Security: Update 2002, TechRepublic,

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

URL:http://itpapers.techrepublic.com/abstract.aspx?kw=%22managing+content+security%22&docid=32822 , Copyright 2002, TechRepublic, Inc.

[18] Burke, Brian E., Content Security: The Business Value of Blocking Unwanted Content, July 2003, URL:http://www.surfcontrol.com/general/assets/whitepapers/BusinessCaseContentSecurity.pdf, Copyright 2003, IDC

[19] Unknown, Manage Junk and Adult Content Mail in Outlook 2002, URL:http://office.microsoft.com/assistance/preview.aspx?AssetID=HA010347791033&CTT=4&Origin=CH010715451033 ,Copyright 2003, Microsoft Corporaton

[20] Violino, Bob, Metrics Prove a Lifesaver, Secure Enterprise Magazine, November 2003, Copyright 2003 CMP Media, LLC

[21] Kennedy, Susan, Best Practices for Wireless Network Security, ComputerWorld, November 10, 2003, QuickLink # 42642

[22] Wack, John, Cutler, Ken, Pole, Jamie, Guidelines on Firewalls and Firewall Policy, January 2002, URL: http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf, Copyright 2002, National Institute of Standards and Technology

© SANS Institute 2004, Author retains full rights.

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

Last Updated: May 23rd, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced