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

Andrew Sippel
GSEC Candidate

Securing Public Access Computers In a Library Setting

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Preamble

The idea for this paper began while I was vacationing in Florida. I had my laptop with me, but the modem wasn't working. With no broadband available, I wasn't able to download a new driver off the web. I ended up going to the local library. I was able to find the file I needed in no time, but it was too big to fit on a single floppy. The idea flashed through my head to email it to myself, until I remembered why I was at the library in the first place.

As it happens IBM has a little utility that will break a file up, and span it across multiple floppies. I was saved, or so I thought. After I downloaded the utility, I discovered I wasn't able to run it because it wasn't an approved application. I struggled with this for some time, until I discovered I was able to run a batch file from a floppy, if it was named 'explorer.bat'. Once I was able to find the spanning application's location on the hard drive, I created a batch file that loaded the spanning application, and passed it the path to the file I needed to span. Mission accomplished, and I was on my way.

All this lead me to thinking about what else I could do. Were there other exploits to be discovered? I checked the computers at three public libraries. The first one was, of course, in Florida. I checked two other libraries once I returned home. The last two were in Upstate New York, in adjacent county library systems. What I found was similar in each location. All three allowed the 'explorer.bat' script to run from a floppy. Using this method I was able to load the command prompt at two libraries, the Florida library having apparently removed, or renamed, the executable. I also discovered the 'autorun' feature was not disabled on one of the New York computers. This computer also did not prevent me from renaming files on the C: drive with the 'explorer.bat' script, even while it prevented me from running 'un-authorized' applications.

This exercise showed me how even a fairly well protected system can be compromised by one simple flaw, and a motivated user.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Preamble 2

Table of Contents 3

Abstract 4

Introduction 5

Physical Security 6

- The hardware: 6
- The environment: 7
- The users: 8

Computer Configuration 9

- The BIOS 9
- The Domain: 10
- The Microsoft Configuration Checklist: 11
- Locking down the OS and File System: 11
- Locking Down with GPOs 13
  - Computer Configuration Policies 13
  - Services 16
  - Internet Explorer (IE) 17
  - All The Rest 18
  - Templates 19

Summary 21

Bibliography 22

© SANS Institute 2000 - 2005, Author retains full rights.

Abstract

The purpose of this paper is to describe ways for public library's to balance information security with free access and user privacy in publicly available computers. It is intended to be a planning guide for both technical and non-technical administrators and may also be used as a tool to review a library's current system. The physical security of a system, and the configuration of the workstations, is central to the successful deployment of a publicly accessible computer. Without securing the computers themselves, and ensuring they cannot be tampered with, the remaining issues regarding this subject may be completely moot. While this paper may be a basis upon which a system administrator can create a secure public access computer, I do not expect it will be comprehensive. It will not discuss such necessities as how to build and configure a Windows Domain, or the various network services needed to sustain a modern computer network, such as DNS, DHCP, etc. Nor will it cover Network security, patch management, or the various legal issues associated with securing a computer system. In the end I expect this paper will provide a well rounded view of various issues which threaten the security of a publicly accessible computer, and the actions which will help better secure it.

© SANS Institute 2000 - 2005, Author retains full rights.

Introduction

The purpose of this paper is to describe ways for public library's to balance information security with free access and user privacy in publicly available computers. It is intended to be a planning guide for both technical and non-technical administrators and may also be used as a tool to review a library's current system. In this age of global and domestic terrorism, the USA Patriot Act, and an ever increasing population of 'script kiddies', public library system administrators face an ever more challenging task: how to satisfy users' expectations, without compromising system security. More over, library system administrators must decide, in advance, how they will deal with the issue of system monitoring, logging and auditing. This is due to provisions in the USA Patriot Act that compel libraries to turn over ANY information records they have upon request, possibly without notice or any demonstration of just cause.

The purpose of a public library is to offer citizens of a community with (relatively) free access to information. Free access, however, does not mean free reign, nor should it. As with any information system, restrictions must be in place to secure not only the information being sought, but the resources needed to provide that information. While the 'Confidentiality' component of Information Security's C.I.A. model is somewhat less important in this setting, the 'Integrity' and 'Access' components are critical.

In a corporate environment users understand they may be watched. The understanding between employer and employee has, by now, settled into an uncomfortable truce. Employees understand who owns the network, and that they do not have the right to free access, nor an expectation of privacy. In a library setting, however, the tax payers own the system, the tax payers are the users, and the users expect both free access and privacy.

The scope of this paper will be limited to public library computers. It will be assumed that the computers offered for use will be desktops, running either Windows 2000 Pro or Windows XP Pro. It will further be assumed the operating systems for these computers will be freshly installed, and that there is a pre-existing network structure to support the new workstations. I will not, therefore, discuss such necessities as how to build and configure a Windows Domain. Nor will I attempt to describe the various network services needed to sustain a modern computer network, such as DNS, DHCP, etc. Any discussion of proprietary databases or online card catalogs will be limited to how they may affect the security settings discussed and their fundamental impact on the users' overall experience. While I will mention various legal issues associated with each of these topics, I will avoid any in-depth discussion. This practical is written for a technical certification, not a legal one.

Even with these limits this paper has a rather large scope. The discussion, therefore, will focus on the following specific topics:

Physical security – This section will be a discussion regarding ways to protect the library's computer hardware, the general environment and the users themselves.

Computer Configuration – This section will comprise the bulk of the paper, and will include anything that may be configured on

© SANS Institute 2000 - 2005 Author retains full rights.

each workstation being offered for public use. This will include BIOS settings, System and NTFS permissions, Active Directory controls, and other related topics.

It should be said at this point that the vast majority of a library's general user base use library computers for purely platonic purposes and intend no harm whatsoever to the system. It can just as easily be said, however, that ignorance is a system administrator's greatest threat. A user can inadvertently, and with no malice intended, do just as much damage as someone who does intend harm. Therefore, I will approach this subject with the intention of preventing all forms of user tampering, without regard for the user's abilities or intentions.

While I expect to present this paper as a basis upon which a system administrator can create a secure public access computer, I do not expect it will be comprehensive to all existing or future situations. It remains the responsibility of the individual system administrator to evaluate the particular needs of the library carefully, apply the recommendations in this paper with due care, and maintain a well patched system. In the end I expect this paper will provide a well rounded view of various issues which threaten the security of a publicly accessible computer, and actions which will help better secure them.

Physical Security

The hardware:

The only people I have ever encountered who question the need for physical security are those who are naïve enough to think people are honest, or have never had anything of theirs stolen or broken by someone else. I'll assume, therefore, that the basic need to secure the equipment is a given. The fact is, if they can touch it, they can take it or break it.

There is no doubt physical security can be a challenge, especially when a system is to be installed in a building built before computer networks were considered for public use. Usually, however, an unused corner in a closet, or office, can be fashioned for use as a server/network closet. If a separate closet is not easily available, a lockable rack, or cage, may be used. The most important idea is that the servers and network equipment should not be easy to get to. Ideally, even the library staff should have restricted access to this equipment.

If you have the luxury of building the entire system from the ground up, select rack mountable servers. This provides the best use of space, and allows for your network gear and any future expansion within the same rack. Make sure patch panels are protected and, wherever possible, cables runs should be installed overhead, using plenum grade cabling. If there is no way to run wires overhead, make sure cables are protected from damage. A solid bump from a cart, or careless kick from a user, can cause a variety of network anomalies. Again, the primary purpose is to make things reasonably inaccessible.

Finally, with regards to the workstations themselves, use cable locks. These are devices that utilize a

© SANS Institute 2000 - 2005 Author retains full rights.

positive connector, combined with a vinyl clad cable, to basically tie the computer and monitor down. The point to using a positive connection is that it forces a thief to break the CPU or monitor case in order to steal it. Besides creating an obvious commotion, the equipment would be much more difficult to sell, or even use. The computer itself should be housed in a way that makes getting at the back of the unit difficult. This will make stealing keyboards and mice more difficult. At the very least keep this point in mind when developing any kind of monitoring system. While precautions are intended to prevent equipment theft, or damage, it should be understood that if someone really wants to steal it, they will likely find a way. But why make it easy?

The environment:

The most basic issue to be resolved when designing a library computer system for public access is its location within the facility being considered. There are several issues to be addressed here including; properly sizing and installing electrical power, determining how users will connect to the Internet, choosing the best kind of counter space, and many others. Also of serious concern is the proper spacing of terminals to meet local fire codes.

The area chosen should be segmented from the rest of the library. The main reason is to prevent people from simply walking up and sitting down, with out first checking in, thereby 'cutting the line'. Besides being fundamentally rude, it can be, and often is, a source of conflict. By segmenting the area, physically, you accomplish two things. First, of course, you eliminate the line jumpers. Just as importantly, however, you gain control over who is sitting down at your computers in the first place. This provides you with the opportunity to record user information, allowing for easier monitoring of the workstations, as well as a more congenial environment.

The area should be laid out so all the computers are visible to either librarians or cameras, with a single entry and exit point. When limiting access careful attention should be made to adhere to local codes for maximum density, and emergency evacuation routes. Surrounding the computers with tall book stacks may be a good way to ensure no one jumps the line, but it is also a serious obstacle when trying to evacuate the area.

For the most part local electrical, building and fire codes will dictate what wiring, materials, and construction techniques should be used to ensure a safe environment. There are, however, some issues that municipalities do not address when it comes to the security of a library's computer network.

Depending on the amount of traffic the computer areas will receive, it may be necessary to have full time supervision of the workstations. The main duty, of course, will be to maintain order among users wishing to access the computer resources. To do this there will likely be a sign up sheet to keep track of who is entitled to use the next available computer. Other duties, however, will inevitably include monitoring the users to ensure no one is attempting to damage or steal equipment. This may be a simple task when there are only a few computers, but becomes increasingly difficult as the number of computers grows.

Another way to monitor the workstations is to implement video surveillance. Installing cameras has many useful advantages, and few disadvantages. Many of the articles I read during my research

© SANS Institute 2000 - 2005 Author retains full rights.

discuss what is called the "Principle of Prevention". This principle states that the likelihood of a crime, or incident, decreases as the overall awareness of a camera's presence increases. In other words, people are less likely to engage in troublesome behavior if they know, or think, they are being watched. For more information on these principles check out:

© SANS Institute 2000 - 2005, Author retains full rights.

Research paper written for police research groups:
http://www.popcenter.org/Problems/Supplemental_Material/Shoplifting/fcpu5.pdf

New Zealand Police policy on CCTV cameras in public places:
http://www.police.govt.nz/policy/cctv.php

Australian Police FAQ regarding cameras in use in public places
http://www.afp.gov.au/afp/page/Prevention/SafetySecurity/PersonalSecurity/CCTV/FAQ.htm

Like most equipment installations it is best to address video monitoring systems early in the design phase, to allow for appropriate power, wiring, control systems, etc. As technology advances, however, so too do the options available for video surveillance. It used to be the only option was a closed circuit co-axial surveillance system which required special designs, with big installation issues, with even bigger costs. Today, however, the choices are plentiful, and getting less expensive every day. Of course there are still co-axial camera systems, which offer a wide array of camera types, and sizes. There are also IP base camera systems, which can utilize the same cat5 cabling the computers themselves use. The advantage with IP cameras is they eliminate the need to run different cables, and can be run along with all the other network cables. USB cameras are inexpensive and, despite distance limitations, may be used to provide the person monitoring with another set of eyes. Wireless cameras, too, are becoming less expensive and more reliable. In the end the physical limitation of the facility, as well as budgetary constraints, will decide what system is most sensible.

The users:

Finally, the users themselves need to be secured. Not secured as in nailed to the floor, tempting as that might seem. The idea here is to be aware of who is using the computer systems. Requiring users to sign-in helps to maintain order among the users and creates a log, which allows for future analysis of trends. Things like busiest days and times or the number of waiting users at any given time can be tracked, which may be used to justify budget requests later.

An important consideration to be made beforehand is to define who is an eligible user. Additionally, if there are to be restrictions how are they to be enforced? Some library systems do not allow anyone who is not a registered library user, often meaning a local resident, to access the computers. In this case a current library card verifies a user's eligibility. If there are no restrictions regarding who is eligible, the question then is will you require any type of identification before a user will be given access?

Once a decision has been made regarding user sign-in, the issue of user logon must be addressed. This can get messy fast, and careful consideration should be given the various problems associated with creating user accounts for the general public. Consider the library I visited in Florida. I am not a Florida resident, and I used the system only once. Add to that the fact that it has been almost two years since I visited that library. Attempting to track library users by creating a logon account for each person that wishes to use the system would end up creating hundreds, or even thousands, of abandoned accounts.

© SANS Institute 2000 - 2005 Author retains full rights.

An alternative to creating user accounts could be to implement smart cards. Here too technology has brought the cost to implement a solution down to reasonable levels. By now most people have stayed in hotels that use swipe cards to open room doors. The same type of system can be used to allow access to a computer. By combining a sign-in sheet, with a list of swipe cards, a user can be tracked according to the swipe card information. Of course there are some logistical issues with getting the cards back, and replacing lost, stolen or broken cards. Overall, however, they create a method to track users, without the boondoggle of individual user accounts.

Computer Configuration

The following discussion describes many configuration changes possible to secure a domain workstation. It is by no means comprehensive. Nor is it intended to imply that ALL changes are inherently necessary. Each setting should be thoroughly reviewed before implementation to ensure its appropriate, and un-conflicted, use.

The BIOS

So let's start with the BIOS, the Basic Input Output System. There are several settings in the BIOS that will go a long away in helping to lock down a computer. The first such setting is the BIOS password. Of all the changes described below, none is safe without a BIOS password. One of the first things the computer will display when booting, is how a user can enter the setup utility (aka: the BIOS). Whether it's pressing the F1 key, the Del key, or some other key, this is the point at which your computer is most vulnerable. Once the BIOS has loaded, changes to it become more difficult, if not impossible. The BIOS password is not susceptible to normal password cracking methods. That doesn't mean there is no way to crack the password. If you allow the computer to be booted from the floppy disk this is really a very trivial matter. For more on cracking BIOS passwords check out http://www.password-crackers.com/index.html The bottom line here is to select a sufficiently complex password so running these utilities becomes too time consuming.

Once an acceptable BIOS password has been set, the next most important setting to configure is the computer's boot order. This is the device order the computer will use when looking for an operating system to load. By default most computer makers will have this option set in the following order: first the floppy disk drive, then the CDROM drive and then the internal hard disk drive. This is, for the most part a VERY bad setup. Even for a home computer, this setting can cause unexpected problems. In a library environment, however, leaving this setting as is can create a vulnerability of unknown potential (If you haven't done it already, checkout the password-crackers website to see a few). The list of exploits is long, and entire careers have been made and destroyed on this one vulnerability. Suffice it to say, by simply changing the BIOS so that the computer can boot ONLY from the C: drive, or hard disk drive, the vast majority of these vulnerabilities are rendered trivial.

From here the decisions get less cut and dried. For the most part the external ports can be disabled. The serial port will likely serve no definable use, as there are fewer and fewer devices that utilize this port. The parallel port too will not likely be utilized. I am assuming you will be providing a

© SANS Institute 2000 - 2005 Author retains full rights.

network available printer for users. Any available onboard audio ports present a very different problem. While it is unlikely you will want to provide speakers for use in a library, users may wish to use headphones. USB ports, on the other hand, present a completely different sort of problem.

The number and variety of USB devices available is astonishing. Everything from mice and keyboards, to wireless network cards and GPS receivers can be connected to a computer via USB ports. Printers, scanners, memory sticks, digital cameras, audio recorders, even gaming systems, and the list goes on and on, can be almost instantly available when connected via an active USB port. While there are ways to limit a user's ability to load device drivers, as discussed later, many devices use drivers native to the operating system. Memory sticks, digital cameras and MP3 players are excellent examples of devices that do not require a driver to be installed.

While it is highly unlikely users will try to bring in their own printer or scanner, the number of people using USB memory sticks and digital cameras has exploded. Add to that the possibility that a motivated user, or a kid testing his limits, could create a back door by installing a USB wireless network card, and the list of vulnerabilities grows rapidly. It is, therefore, imperative that a conscious decision be made regarding whether these ports will be left active. The only real advice I can offer is to disable the ports, and see how many people complain. Just make sure the people monitoring know how to answer users' complaints.

The only remaining devices that could cause trouble are the floppy and CD-ROM drives. These are two devices that users will almost always look for. While the use of floppies has dropped, they are by no means extinct. Their usefulness persists for transporting files, and it would be a mistake to assume library users don't use them. CDs have become a mainstay in the computer world, and there are simply too many uses to list here. Library users will, almost certainly, require access to a CD-ROM drive. The bottom line is to find a way to restrict what a user can do, without denying access to the drive entirely. I'll attempt to address this in the section describing Group Policy Objects (GPOs).

One possible alternative is to create a series of CD-ROM and floppy drives connected via USB to a central server, then shared as mapped drives to the individual workstations. This is by far the most expensive way to go as it requires investment in the external drives, as well as all the necessary cabling, active hubs and expansion cards to connect them to a server. There are several benefits to this setup, however. First is total control over what access a user has to the drive media. Because the device is controlled by a remote server, and not the individual workstation, very strict permissions may be set. Another advantage is the ability to log details about the information that was accessed. Among the most important advantages to this method is that by not having these devices built into the workstation there is no way they can be used to boot the computer. Theft, on the other hand, becomes an even bigger concern. Unless special consideration is made, and secure housings implemented, this may be far too expensive to be realistic. After careful consideration a well designed GPO may provide the control required.

The Domain:

Having mentioned GPOs (Group Policy Objects), I need to re-iterate that I am assuming there is a domain structure already in place. By not implementing a domain, administrators will be forced to

© SANS Institute 2000 - 2005 Author retains full rights.

use the workstation's local settings to manipulate user rights and permissions. This has obvious disadvantages, not the least of which is inconsistency between computers or the potential for administrators to lock themselves out should a policy be misapplied. Once the operating system has been installed, the computer should join the domain to facilitate support for central administration. If the libraries administrative workstations are part of the same domain, a separate Organizational Unit (or OU) should be built to contain the workstations that will be provided for public access. This will allow for separate control of each group of computers.

The Microsoft Configuration Checklist:

Microsoft has begun to come clean with regards to the realities of information security. Long maligned as apathetic towards securing their systems, Microsoft now has an overwhelming variety of resources available to administrators. Some excellent How-to documents are available from the Windows 2000 Security Hardening Guide at:

http://www.microsoft.com/technet/security/checklists/default.mspx

Another excellent document Microsoft has available through their 'Hardening Guide" is the Security Configuration Checklist., which can be found at:

http://www.microsoft.com/technet/security/prodtech/Windows2000/win2khg/appxc.mspx

This checklist is a list of security settings available through either the local, domain or GPO policies. It should be printed and used to assist with crosschecking for policy completeness and conflicts.

Several other pages linked from these pages offer guides for securing the various subsystems within a windows domain including; Active Directory, Operating System Configuration and Configuration Tools and Templates.

While these pages will not always take you by the hand and walk you step by step through the entire configuration process, they are an invaluable resource for learning the details surrounding the major components of securing a Windows system. The main purpose of these guides is to help build a well rounded understanding of the capabilities of Group Policies, and the flexibility they offer administrators. In the following sections I will begin to address the more specific components these web pages discuss.

Locking down the OS and File System:

By now there are few in the IT world that are unaware of the insecurities of a FAT or FAT32 formatted partition. It should, therefore, be a foregone conclusion that NTFS will be the file system of choice. The discretionary access control lists built into the NTFS file system are the basis for security on a Windows domain workstation. Since we will be mainly concerned with securing computers from the local users, I will not address the access control lists associated with shared folders, the concepts of permission inheritance or of effective permissions. I'll assume that the developers of the Domain, or proprietary applications, have secured the servers appropriately, and that there will be no user shares on the public workstations.

© SANS Institute 2000 - 2005 Author retains full rights.

The workstations themselves should have a minimal set of accessories and add-ons, leaving only those truly needed. Applications and add-ons should be re-added only after careful consideration and sufficient user complaints. Special desktop themes, mouse pointers and document templates will likely cause more trouble than they are worth. Applications like 'paint', 'calculator' and the various card games that come with the operating system are relatively harmless. Internet Explorer, while much maligned and chock full of vulnerabilities, will be the most used application on the computer. Outlook Express, Windows Media Player and Windows Messenger, on the other hand, should be thoroughly avoided. These open a wide variety of holes to maliciously coded web sites and are a favorite target for hackers.
(For more information go to www.google.com and enter any of the above mentioned application names, followed by 'exploit' and get ready to do ALOT of reading).

The remaining applications and services that can be included at installation will have varying degrees of usefulness. Utilizing the Indexing Service is one that will depend on the individual library's needs. This is a handy service for use with online card catalogs and searchable websites, but will serve little purpose otherwise. The same is true for the Management and Monitoring Tools, Networking Services and Other Network File and Print Services. While there may be specific reasons for using these, they should be carefully considered before being installed.

There are some important differences between the way a Windows 2000 computer and a Windows XP computer use the file system by default. Windows 2000, unlike Windows XP, gives the 'everyone' group 'Full Control' by default. This includes the security settings of the system drive (often the C: drive). If the drive or folder is not shared this may be acceptable for securing network access , but gives local users the keys to the proverbial kingdom. It is, therefore, imperative that after the initial installation has finished administrators return and change this setting. My opinion is that only the local 'Administrators' and the SYSTEM groups get full control of the system root drive. Depending on the structure of your IT department, however, you may include additional local groups with lesser permissions in order to facilitate layered security among library staff. Any Domain level groups should be added to local groups for the purposes of granting permissions.

This brings me to AGULP; not a nervous jugular reflex, a method for applying permission. The term AGULP stands for 'Accounts', 'Global', 'Universal', 'Local', and 'Permissions', and is applied as follows;

> *Accounts* are put into *Globa*l groups which may, in turn, be put into *Universal* groups; global and/or universal groups are put into *Local* groups and these local groups are assigned the prerequisite *Permissions*.

Therefore, it should never be necessary to assign a user account with permissions to any given resource. Since we are talking about accessing the system root drive, it would be even less likely to find groups like 'Everyone' or even 'Domain Admins' assigned specific permissions. Limiting the 'Everyone' group prevents un-authorized access to the drive by users that may not even be part of your domain. By avoiding the over use of the 'Domain Admins' group, you make it more difficult for attackers to enumerate permissions.

© SANS Institute 2000 - 2005 Author retains full rights.

One last thing to address with regard to the operating system is the OS/2 and POSIX sub-systems. If there is to be no integration between your public computers and systems running either OS/2 or POSIX it is important to remove this support. To do this will require changing the registry. Windows 2000 has registry entries for both the OS/2 and POSIX systems. The first place is in

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT

you will need to delete all values within this key. The next place to look is in:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SesionManager\SubSystems

Delete the key entries for POSIX and OS/2. As with ANY registry changes it is important to review each in advance and be sure you are not creating problems. According to Microsoft (article Q308259) Windows XP does not support either OS/2 or POSIX. Just to be sure, however, I recommend checking the above registry keys and confirming there are no references. If you are like me you'll run a full registry search for both 'OS/2' and 'POSIX' before you're satisfied.

Locking Down with GPOs

Windows 2000 and Windows 2003 domains have similar management applications. However, there are some minor differences with the interfaces themselves. Below is an example of how a Windows 2000 GPO looks, compared to a Windows 2003 GPO:

Windows 2000	**Windows 2003**
Prevent users from installing printer drivers	Devices: Prevent users from installing Printer drivers

Notice the prefix 'Devices:' for the Windows 2003 example. The policy itself, however is the same. While this is not true for every policy, they are close enough that you ought to be able to connect the dots. I will be using the Windows 2003 format, as that is the system I have to work from.

To look at the Default Domain Policy without some idea of its abilities and purpose, is to be immediately overwhelmed and confused. The shear number of items available for configuration is awesome. Without a general understanding of its complexities, attempting to make changes would provide a fast track to lunacy. This section, therefore, is NOT intended to be a dissertation on GPO's, but rather an overview in order to provide a framework within which to prioritize and evaluate important settings. The details I will discuss are those items that directly affect the user's ability to tamper with library resources, as well as ways to limit computer functionality. Once again it is important to note that each setting should be thoroughly reviewed before implementation to ensure its appropriate, and un-conflicted, use.

There are several levels at which policies can be applied; locally on each computer, globally throughout the domain, or according to Organizational Units within the domain. The locally applied policies, however, are inefficient in some fairly significant ways. First of all, they require administrators to access each machine individually which leaves open several liabilities, as stated earlier. Just as important is the fact that the variety of controls available at the OU and Domain level

© SANS Institute 2000 - 2005 Author retains full rights.

are not available at the local level. As a result I will not discuss locally applied policies. All the policies discussed will be available at both the Domain and OU level, so I will not recommend one application over another. I'll assume these decisions will be made on a case by case basis.

Computer Configuration Policies

The first item I want to address are the Account policies. This is the group of policies under 'Computer Configuration > Windows Settings > Security Settings'. The policies involving Password and Account Lockout are not going to provide much by way of securing a public computer. These settings should, however, be applied to the library's administrative computers, to ensure librarians maintain due diligence in securing the non-public systems. Unless you have decided to create a new user account for each public user, and are ready to reset passwords constantly, these settings will do little for you.

The Local Policies will, however, provide several useful settings. Auditing should be enabled for all computers to track user attempts to change policies, or access directory services. Assuming you will NOT be requiring individual user logons, auditing logon events would be useless. This may not be true, however, if you choose to implement Smart Cards. Users may then be tracked using the information on this card. Auditing privilege use, too, can provide valuable alerts to users attempting to make system changes. Events like an attempt to add the 'Everyone' group to another group should generate logs entries. The main issue you will encounter here is the requirement to maintain the logs. Depending on how many computers you will monitor, you may have quite a task trying to sift through the logs for the grains of sand that say 'someone broke in'. I won't get into the many different Audit log utilities. Besides the variety of ways in which they can be used, the subject accounts for its own GIAC certification. Suffice it to say, you should be prepared to invest plenty of time in either reviewing your logs, or choosing an application to help you audit your logs.

One other item regarding logging is enforcement. If you have a policy and you fail to enforce it, you really don't have a policy. This means that if you choose to audit you user activities, you MUST review you logs, AND take action against violators. Another important issue regarding any user records kept, including audit and proxy logs, user sign in sheets, etc, is the USA Patriot Act. There are provisions in this law that compels library system administrators to turn over audit information upon request. The legal standards that law enforcement must meet has been set very low, and may require nothing more than confirming the identity of the requestor as a law enforcement official. Recent court cases have overturned some parts of this law, and there are no doubt many cases yet to be heard. Regardless, you should work closely with your legal counsel when it comes to developing audit policies.

Another serious concern is deciding whether to overwrite entries when the log has filled up. This can be minimized by making some changes to the log file sizes, and even to the log file locations. The GPO available to make these changes is in - Computer *Configuration > Windows Settings > Security Settings > Event Log*. Settings include log sizes, retention method and days to retain entries before they get overwritten. There is no setting for the log file location, however. In Windows XP this setting may be changed through the specific log file's properties page in the Event Viewer. Windows 2000, on the other hand, requires a registry edit. This registry entry is found in:

© SANS Institute 2000 - 2005 Author retains full rights.

HKey_Local_Machine\System\CurrentControlSet\Services\Eventlog\%log name%

Change the %log name% to the specific event log you're interested in relocating. You should see a REG_EXPAND_SZ key with a value like '%systemroot%\system32\config\%log filename% (where %log filename% is either SysEvent.evt, SecEvent.evt, DnsEvent.evt, etc.) Changing this setting, and rebooting the computer will move your event logs. For more information on this check out Microsoft's Technet article:

http://www.microsoft.com/technet/security/prodtech/Windows2000/w2kccadm/auditman/w2kadm26.mspx

The next sets of policies are the 'User Rights Assignment' policies. Here is where you will define the basic parameters which will govern such things as; who has permission to shut down the computer, whether anyone can access the computer over the network, or who may logon on locally. Most of these are setup when the OS is installed, but a familiarity with these settings is important to be sure no un-deserved access is inadvertently granted. For example, the 'Everyone' group should not appear anywhere in the list of permitted, or denied, groups. Obviously permitting 'Everyone' to do anything is bad. The flip side to that is that if 'Everyone' is denied, you are too, potentially locking you out of your own computer.

Most of these policies are fairly self-explanatory, so I won't spend anymore time discussing them. Suffice it to say this is a section you will want to review thoroughly, including how the policy behaves if it is 'Not defined'. A policy that is enabled but has no group assignments can often be used to better advantage than one that is simply 'Not defined'. Several policies are 'no brainers'. You should define the 'Add workstations to the Domain', 'Change the system time' and 'Load and unload device drivers' policies, assigning only the local 'Administrator' group.

The Security Options is the last group of policies under 'Local Policies', and has several that are not simply important, but may be legally required. First, change the Administrator and guest account usernames. This is just good sense. The guest account should be disabled, unless it is to be used as the default user account. If the local administrator's user account is to be left enabled, it is important to realize it cannot be locked out by consecutive incorrectly entered passwords. This leaves the door wide open to scripted attacks on the administrator account. By changing the administrator's username, the difficulty in hacking the account by brute force is increased exponentially. A better idea altogether is to use the policy labeled 'Accounts: Administrator account status', setting it to 'disabled' and using domain level accounts for all administration tasks. Now your 'script kiddies' can try to break the administrator's password all day and you have no worries.

The policies on Audit and DCOM are mainly for workstations in sensitive security environments, and will offer little to library administrators. The policies on devices, however, should be reviewed carefully. Also the rules governing the installation of printers and 'Unsigned' drivers may be set here. The Domain controller and Domain member policies are outside the scope of this paper.

The 'Interactive logon:' settings for 'Do not display last user name' and 'Do not require CTRL-

© SANS Institute 2000 - 2005 Author retains full rights.

ALT-DEL' are your call. Be careful to verify these do not conflict with the next two; 'Message title…' and 'Message text…' which should absolutely be enabled. These refer to the warning box users will see before they are given access to the computer. By clicking the 'OK' button, users are at least confirming they saw the message, even if they failed to read it. The message should be short and easily understood. The main idea should be a brief description of the library's acceptable use policy. The actual message displayed should be reviewed by your legal counsel to be sure it is both clear and enforceable.

If you will be using smart cards, interactive logon policies will help to define their implementation. The main setting is what will happen if the smart card is removed; No action, Lock workstation or Force logoff. There is a 'gotcha' here. If you are running Windows 2000 you cannot have a screensaver configured. If the screen saver kicks in before the smart card is removed the policy will not cause the desired action. I was not able to find any information indicating this is a problem with Windows XP, but it's always a good idea to test and be sure.

Services

The next items to address are the system services settings. Here Windows 2000 GPOs differ slightly from Windows 2003 GPOs due to some services being named differently and some simply not existing. Windows 2000, for example, offers settings for the 'Internet Connection Sharing' service, while Windows 2003 offers the 'Windows Firewall/Internet Connection Sharing' service. Windows 2003 offers settings for the 'Error Reporting Service', while Windows 2000 has no such option available. The bottom line is to be thorough, and verify.

So which services should be forced to what settings? Here again, the answer is 'It depends', not just on your particular system, but also on whose advice you choose to take. I used the Microsoft Press publication 'Microsoft Windows Security Resource Kit' as a reference on this. Some services installed by default are fairly dangerous services to have running in this type of environment. Below is a list of services that you should seriously consider disabling:

Event Reporting – Used to send application error reports to Microsoft. This service is non-essential, and can cause some user confusion. If needed, due to application performance problems, it can be enabled for troubleshooting, then off once the issue is resolved.

IMAPI CD-Burning Service – (XP only) This allows users to utilize CD burners. It is not advisable to offer CD burning services on a publicly accessible workstation. If necessary you might consider setting up a CD burner on the monitor's PC, and offering it as a service.

Messenger – This service is similar to the AOL Instant Messenger or MSN Messenger, but includes automatic messages sent from printer spoolers or other third party messaging software. It is a target of malicious coders, and will not affect system performance if disabled.

Netmeeting Remote Desktop Sharing – This service is not inherently insecure, but it is

© SANS Institute 2000 - 2005 Author retains full rights.

entirely un-necessary in a library environment. It is used to allow remote users to take control of the currently logged on user's desktop, and disabling it is strongly recommended.

Remote Registry Service - This service is used by administrators to modify a computer's registry remotely. It can be a VERY useful service, but can be exploited. The primary ability lost by disabling this service is the inability to scan a remote computer using Microsoft's Baseline Security Analyzer, or several other utilities which check for missing system patches. Here again it is beter to leave it off, except when needed.

Routing and Remote Access – This service is used to forward TCP/IP packets. Disabling this service will seriously impair the creation of a network backdoor. Since the workstations should not be used for routing purposes anyway, disabling this service will not effect performance in the least.

SSPD Discovery Services (XP only) – This is the service used to install Plug-n-Play devices. Disabling this service will prevent the system from recognizing new devices that a user may try to connect. This is the point at which you should carefully consider your user base, and their particular needs, as this will prevent the system from automatically mounting USB devices.

Telnet – This is amoung the most dangerous services to leave enabled. Even set to manual this service could be compromised. If you disable only one service, this should be it. The telnet service provides a user with command line access to the computer, allowing a sophisticated user the ability to run commands remotely.

Terminal Services – Available on Windows XP workstations, this service is similar to both the Telnet and Netmeeting services. Disabling it should be considered as critical as the other two. The is no reason a remote user be able to connect to a workstation, ever.

Wireless Zero Configuration – This service supports automatic configuration of wireless network adapters. When combined with the SSPD Discovery Service, and an active USB port, this service could easily enable someone to create a wireless backdoor.

Internet Explorer (IE)

Internet Explorer (or IE), as stated earlier, will be the most used application on your public access computers. There are a wide variety of web browsers that do the same things as IE, and some are significantly less vulnerable to malicious websites. The reality is, however, more people are familiar with IE than any of the others. A well patched version of IE should be plenty sufficient, and will

© SANS Institute 2000 - 2005 Author retains full rights.

generate fewer user complaints than an application most have never used. As a result, sticking with IE will likely create the fewest headaches in the long run.

Having said that, it is important to remember two things about IE; first, it is probably the most targeted application running on the Internet, and second without expending the effort to lock down some settings it is only a matter of time before it is the root of a major incident on your network. As a result I am going to address Internet Explorer separately from the remaining GPO settings.

First I assume you are using a proxy server to manage web traffic. If you're not, shame on you, you should be. It doesn't matter much which proxy you choose as long as it is reliable and you keep it properly patched. Unless you are offering web services to the outside world, there is really no need to have an expensive, high end proxy server.

There are several settings to configure to properly setup IE to access your proxy server. The first is in '*Computer Configuration > Administrative Templates > Internet Explorer*'. Find the policy labeled 'Make proxy settings per machine (rather than per user)'. This will prevent the user logged on to change any of the settings that follow.

Next, under '*User Configuration > Windows Settings > Internet Explorer Maintenance > Connection*' find the Proxy Settings policy and right click on it, and chose 'Properties' from the menu. This is were you will enter the IP (or NETBios name) of the server offering proxy services. You will most likely leave the 'Use the same proxy server…' check box checked.

The next policy you may want to address, 'Disable changing proxy settings', is under '*User Configuration > Windows Components > Internet Explorer*' GPO. This is similar to the 'Make proxy settings per machine (rather than per user)' described above, but is implemented per user, making it that much more difficult for a 'script kiddie' to cause trouble. Also under this GPO is 'Disable changing home page settings'. Disabling this may be annoying for some of your users, but will help when a malicious website, cookie, or web script, tries to change the home page. Under 'Internet Control Panel', in this same GPO, you should disable all the property pages listed. This will prevent the unauthorized alteration of your settings.

There are certainly plenty more settings to look into before you can be confident IE is sufficiently locked down. You may have preferences regarding what your IE menus to offer, or how specific security features operate. As always, do your home work before implementing a setting.

All The Rest

In the interest of brevity, rather than explain each of the following settings, I will simply list them, with their recommended setting to the right. Once again, I am not indicating these settings are necessary in every situation, nor that none will conflict with any other. The intention is to show those policies which will have the greatest impact on the overall security and stability of your systems. Each of these should be thoroughly reviewed and understood before implementation. In addition the policies which I do not address here (and there are hundreds of them) should be reviewed to ensure an appropriate policy for your system is not overlooked.

© SANS Institute 2000 - 2005 Author retains full rights.

Under '*Computer Configuration > Administrative Templates > Windows Components'*

Application Compatibility – Prevent access to 16-bit applications (enabled)
Internet Information Services – Prevent IIS installation (enabled)

Under '*Computer Configuration > Administrative Templates > System'*

Turn off Autoplay (enabled)

Group Policy – Turn off background refresh of Group Policy (disabled)

Under '*User Configuration > Administrative Templates > Windows Components'*

Application Compatibility – Prevent access to 16-bit applications (enabled)

Start Menu and Task Bar – Remove licks and access to Windows Update (enabled)
- Remove My Documents icon from start menu (enabled)
- Remove Favorites menu from Start Menu (enabled)
- Remove Search menu from Start menu (enabled)
- Remove Help menu from Start menu (enabled)
- Remove Run menu from Start menu (enabled)
- Remove My Network Places icon from Start menu (enabled)
- Prevent changes to Taskbar and Start Menu Settings (enabled)
- Lock the Taskbar (enabled)
- Remove user name from Start Menu (enabled)

Desktop – Remove My Documents icon on the desktop (enabled)
- Remove My Computer icon on the desktop (enabled)
- Remove Recycle Bin icon on the desktop (enabled)
- Hide My Network Places icon on the desktop (enabled)
- Don't save settings at exit (enabled)

Control Panel – Prohibit access to the control panel (enabled)
- Display – Prevent changing wallpaper (enabled)

- Printers – Prevent addition of Printers (enabled)
- Prevent deletion of printers (enabled)

System – Prevent access to the command prompt (enabled)
- Prevent access to registry editing tools (enabled)
- Run only allowed Windows Applications (enabled)

Ctrl+Alt+Del Options – Remove Lock Computer (enabled)
- Remove Change Password (enabled)
- Remove Logoff (enabled)

So far I have discussed ways to prevent users from doing things. What I have not discussed is what users will be allowed to do. After all, if you are going to offer a computer for anyone to use, it ought to be able to do something useful. Internet Explorer is a no brainer, provided it is patched

© SANS Institute 2000 - 2005 Author retains full rights.

and locked down there shouldn't be too many problems. With all the above described BIOS changes, services disabled, a secured file system in place, and a well designed GPO, you'd think you'd be good to go. The problem is, I still haven't addressed that 'explorer.bat' loop-hole that got this whole paper started. The policy which will prevent this is the 'Run only allowed Windows Applications' listed above. What is important to remember here is to include not only the application name, but the authorized path to the application as well. This will prevent the user from running any applications off a floppy disk or CD. Some users will inevitably complain they can't run their favorite game, or access a certain media player, which may be solvable by either incorporating the application into your systems, or finding one that is already installed that works. In the end, however, the 'script kiddie' and the motivated user will have to keep looking, or move on.

Templates

All this is not to say you should start building GPO's from scratch. Microsoft provides several sample templates for both servers and workstations. These templates range from minimal to paranoid security, and can be used to gain valuable insights into the various GPO settings. There are three basic templates available; 'compatws', 'securews' and 'hisecws'. The 'compatws' template is basically what is set by default, with some loosening of restrictions on the 'users' group. The main purpose of this template is to provide a usable platform where the default user permissions are too restrictive creating compatibility issues with some software. You will only need this type of policy if you have an older online card catalog, or database. The providers of those applications can advise you as to their particular needs. The 'securews' and 'hisecws' templates apply increasing levels of control over such items as account policies, communication between client and server, what protocols to use for authentication, and much, much more. For details on these templates checkout Microsoft's web site:

http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/windows/xp/all/reskit/en-us/prdd_sec_umgs.asp

The National Security Administration, too, has several templates available for download at:

http://www.nsa.gov/snac/downloads_win2000.cfm?MenuID=scg10.3.1.1

Another useful tool Microsoft provides is the Configuration and Analysis Tool Plug-in available for the Microsoft Management Console. This utility is designed to compare policy settings against existing and hypothetical configurations. While this tool has the ability to implement policy settings, I don't recommend using this function as there may be unnoticed, or unintended, changes that can have adverse effects. This tool should be used for comparison purposes only, unless you are absolutely sure you have reviewed all the settings.

Another utility worth looking into is the 'Secedit' utility. This is a command line utility which offers a multitude of control options for applying, analyzing, exporting, validating, and refreshing policies. This can be very useful for auditing or analyzing computers, as well as for scripting changes across many computers. Like most Windows based utilities, however, secedit.exe must be run locally, or from a terminal services session, as there is no remote computer function. The

© SANS Institute 2000 - 2005 Author retains full rights.

version of secedit in Windows XP has replaced the /refreshpolicy switch with the gpudate command. Gpupdate offers administrators the ability to refresh policies on remote computers using the '/Target:{Computer | User}' switch. There are several other useful options including forcing user logoff, forcing computer reboot and forcing the computer to load policies synchronously the next time the computer reboots.

© SANS Institute 2000 - 2005, Author retains full rights.

Summary

The physical security of a system, and the configuration of the workstations, is central to the successful deployment of a publicly accessible computer. Without securing the computers themselves, and ensuring they cannot be tampered with, the remaining issues regarding this subject may be completely moot. The layout of the computers, design of the environment and implementation of user sign-in each provide fundamental protections for your system. The implementation of comprehensive policies, either at the Domain or Organizational Unit levels, provides assurances that users will not un-intentionally alter your systems. In addition, these steps taken together will prevent a majority of the meddling caused by the average hacker.

As with any security issue it is imperative that the most recent documentation be reviewed to ensure nothing is overlooked. This paper was written to address the unique security concerns surrounding publicly available workstations in a library. As stated earlier, there is no way to know all the circumstances for every possible deployment scenario. It will always be the responsibility of the people building the system to make the final decisions.

Having said that, however, there are some fairly standard procedures needed to provide a fundamentally secure computing environment. I addressed these items in no particular order of importance, opting instead to order the paper according to the context within which each issue should be viewed. Unfortunately the scope of this paper did not cover many other issues involved in designing and maintaining a secure computing environment. Network Security, Patch Management, Legal Requirements, and more, would need to be considered when building a network of this type. The full scope of this topic could easily be expanded to fill a book (and a pretty thick on at that).

© SANS Institute 2000 - 2005 Author retains full rights.

Bibliography

Internet References

Infopeople - *Library Computer and Network Security* - ©November, 2004 Infopeople Project.
http://infopeople.org/resources/security/

Newby. G. B. – *Information Security for Libraries* – School of Information and Library Science University of North Carolina at Chapel Hill
http://www.petascale.org/papers/library-security.pdf

Podesta, J. - USA Patriot Act: The Good, the Bad, and the Sunset – American Bar Association
http://www.abanet.org/irr/hr/winter02/podesta.html

Minow, M - *The USA PATRIOT Act and Patron Privacy on Library Internet Terminals* - February, 2002. Available at:
http://www.llrx.com/features/usapatriotact.htm

Ekblom, P. – The prevention of Shop theft: an approach through crime analysis - 1986
http://www.popcenter.org/Problems/Supplemental_Material/Shoplifting/fcpu5.pdf

Robinson, R. Crime Prevention Cameras (CCTV) in Public Places - ©2005
http://www.police.govt.nz/policy/cctv.php

Australian Police - Closed Circuit Television Cameras FAQ - ©2005
http://www.afp.gov.au/afp/page/Prevention/SafetySecurity/PersonalSecurity/CCTV/FAQ.htm

CKnow.com – *System Sector Viruses*
http://www.cknow.com/vtutor/vtsystemsector.htm

Mircosoft Technet Articles

Audit Management – *Change the Default Event Viewer Log File Location* - ©2005 Microsoft Corporation. Available at:
http://www.microsoft.com/technet/security/prodtech/Windows2000/w2kccadm/auditman/w2kadm26.mspx

Knowledge base article Q122221 – *How to Protect Boot Sector from Viruses in Windows* Microsoft Corporation; May, 2003. Available at:
http://support.microsoft.com/default.aspx?scid=kb;en-us;122221

Microsoft Windows 2000 Security Hardening Guide

Overview - ©2005 Microsoft Corporation: Available at:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Chapter 5 - Security Configuration - ©2005 Microsoft Corporation. Available at:
http://www.microsoft.com/technet/Security/prodtech/win2000/win2khg/05sconfg.mspx

Chapter 6 - Windows 2000 Hardening Guide Configuration Templates - ©2005 Microsoft Corporation. Available at:
http://www.microsoft.com/technet/Security/prodtech/win2000/win2khg/06tmplts.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

Appendix B - User Rights and Privileges - ©2005 Microsoft Corporation. Available at: http://www.microsoft.com/technet/Security/prodtech/win2000/win2khg/appxb.mspx

Appendix C - Windows 2000 Security Configuration Checklist - ©2005 Microsoft Corporation. Available at: http://www.microsoft.com/technet/Security/prodtech/win2000/win2khg/appxc.mspx

National Security Administration Guidelines

Operating System Guides – Microsoft Windows 2000 Guides- ©2005 Microsoft Corporation. Available at: http://www.nsa.gov/snac/downloads_win2000.cfm?MenuID=scg10.3.1.1

Guide to Securing Microsoft Windows 2000 Group Policy- ©2005 Microsoft Corporation. Available at: http://www.nsa.gov/snac/os/win2k/w2k_group_policy_toolset.pdf

Printed References

Smith, B. and Brian Komar – *Microsoft Windows Security Resource Kit.* - Microsoft Press – 2003

© SANS Institute 2000 - 2005, Author retains full rights.