Security for Small and New IT Departments: Get Your Big Rocks In First

Greg Rolling

Security for Small and New IT Departments: Get Your Big Rocks In First
Greg Rolling
July 13, 2001
Security Essentials ver. 1.2e

Introduction

With today's shortage of competent professionals in the information systems industry, many of us find ourselves wearing many hats in our company's IS department. Often times we are faced with the challenge of having to fulfill roles of System and Network Administrator, DBA, hardware specialist, application specialist, helpdesk operator and security officer all in the space of a few hours within a single day. Others may find themselves working for a company that is increasing in size, and because they know more about computers than their manager, are faced with having to secure an ever-growing network. This paper will attempt to assist the small/single-person IS department in setting up and maintaining a secure environment while filling the many roles necessary to the company.

Big Rocks

There is a story that likens time management to fitting rocks in a jar. The narrator places big rocks in first, then increasingly smaller rocks in the jar. After each addition of stones, he asks the audience if the jar is full. Pouring sand into the jar, the crowd agrees that the jar is officially full only to chuckle as he pours a pitcher of water in over the top of everything. When asked the moral of the story, one person says that "there are gaps in your time and if you work really hard you can always squeeze more into a day." While that is true, the speaker tells us that the real moral of the story is that if you hadn't gotten the big rocks in first you wouldn't have gotten them in at all. When dealing with limited IT resources, it is important to identify and get our "big rocks" in first as well.

Policies and procedures are where we must begin when discussing the idea of getting your big rocks in first. If you don't have a thorough, easy to understand information security policy most of what we will discuss is pointless. There is more involved in writing good policy than this paper will be able to address, but for help with getting your policy going visit Michelle Crabb-Guel's list of sample policies[1] from her SANS course "Building an Effective Security Infrastructure." Of particular interest for those starting from scratch would be "Acceptable Use Policy" and "Network Connection Policy." These documents are very straightforward, easy to understand and a good beginning point for your own customized security policy.

Password management is one of the most basic of security practices. How many times have you been taken off important work in your daily routine to reset a forgotten password? How many times have you visited a workstation only to find the dreaded "Post-it" notes stuck on the monitor with the last six months' worth of passwords scrawled out on it for the world to see? Our inability to control all environment variables makes this a difficult and often frustrating experience both for system administrators and

end users alike. The end users' frustration often stems from passwords being difficult to remember because they are overly complicated, change often, or they must remember different passwords for different systems. As administrators, what could possibly be more frustrating than someone opening Mack-truck-sized holes in the network we spend countless hours securing?

Often trying to keep passwords secret is not enough. One option for helping to secure our network resources is through multiple forms of authentication. Token-based authentication requires the use of a physical token such as a smart card or USB token device. Biometric devices such as fingerprint or retina scanners in conjunction with a strong password also increase security considerably. As of late, this technology can be implemented at a cost as low as $50 per user and may be a reasonable solution for high-security networks. Often times, though, we are part of small IT departments due to lack of available funds and it is difficult to convince check-writers of the inherent value of *James Bond-ish* retina scanners. In this instance, one can only secure their passwords accordingly and do the best job with the available resources.

Passwords are typically stored using encryption on each computer. The location and type of encryption will vary depending on the platform you use. But just because the information is encrypted, don't be lulled into a false sense of security. Weak passwords on a compromised server can literally be cracked in minutes using tools such as L0phtcrack, Crack, or John the Ripper. To avoid this scenario, write into your policy a description of and requirements for passwords.

A good password is going to have many qualities, beginning with length. Obviously, a long password is going to be more difficult to crack than a short one. One thing to consider is using easy to guess words that can be decrypted and cracked using a dictionary attack. This attack involves taking a list of words, running it through a hash algorithm and comparing it to the hashed values contained in the password list. A match equals instant access to your system. A hybrid attack, which places numbers at the beginning or end of words from the dictionary file is a variation of the dictionary attack that is quite effective.

A brute force attack works on the password one character at a time. While this is the most time consuming, it will always be successful. This is where length matters most. The longer the password, the longer it will take a brute force attack to crack the passwords. For instance, using 5 lower-case letters only yields a possible 11,900,000 passwords. Increasing that to 7 lower-case letters yields 8,030,000,000 passwords combinations[2]. Add a combination of upper-case letters, numbers and punctuation marks to the formula and the number increases exponentially.

It is a good idea to download a password cracking program such as L0phtcrack for Windows(trial version available at http://www.atstake.com/research/lc3/download.html) or John-the-Ripper for *NIX (available at http://www.openwall.com/john/) to run against your own systems. That way you can find out exactly how long it would take an attacker to crack your password lists. From that information you can determine how often you

should require your users to change their passwords. If your password is changed before a cracker can feasibly break the encryption, you have increased the security of your system effectively. Good password policy will expire passwords after a set amount of time, and restrict users from reusing the same password again and again. Also, accounts should be set to lock users out after a set number of failed logon attempts. Multiple failed authentication attempts will usually indicate either a need for more user training or somebody trying to gain access to the system by running multiple passwords against a given account. Recommended validity of a password is 30 days for high-security networks, and 90 days is generally thought to be an acceptable maximum. Of course, you run the risk of users writing down their passwords if you expire them too often, thereby reducing your security to a piece of paper taped to the bottom of a keyboard, so striking a balance here may be tricky. Some general guidelines for password policy that can be tailored to your specific needs are:

-length should be a minimum of 7 characters
-should contain a mix of lower-case, upper-case, numeric and punctuation
-names, birthdays, holidays should be prohibited
-words from any language should be prohibited, also
-should expire every 30-90 days
-the more passwords remembered by the system, the better. 6 should be good
-accounts should lock out after 3-5 failed attempts

All this considered, one of the greatest weaknesses in your network will always be the people using it. Whether from intentional destruction or innocent mistakes, the people we support need to be educated in computer security. Training users in effective password management will save the small department hours of work and headache. Make sure they know not to share passwords or leave their machine logged on and unattended. Always lock a console when getting up, no matter how short a period of time they expect to be gone. That guy walking around in the coveralls with a clipboard just might be an "3vi1 haxx0r."

Another very important and critical aspect of limiting access to your network is a good **firewall**. A network firewall is typically a computer or router through which all traffic to and from your network will pass. Safety is balanced with functionality through the use of rules either restricting or permitting access. Unless you are extremely knowledgeable in firewall construction, or have time to study, research and implement this yourself you may want to consider letting a firewall specialist handle this mission-critical set up . The section on outsourcing later in this paper will give some good guidelines to selecting and working with outside help.

But a good firewall is by no means the panacea of perimeter protection. A popular phrase in the organization I work with is "If you don't have **physical security**, you don't have ANY security." Servers should be kept in temperature and humidity controlled, locked rooms with keyboards and monitors hidden from plain sight if possible. Access to these rooms should be monitored with key card access that logs entries, and video cameras where possible. Also, don't forget a good chemical fire extinguishing system.

Water fire extinguishers, such as sprinklers, are good only for backup to save the building in the event of an emergency.

If an intruder should gain access to your network it is best to have ALL machines protected to some degree. There are a number of barriers we can implement to provide us with defense in depth. If you maintain an NT network, set the logon banner to pop up with a warning message that unauthorized use of a computer system will result in criminal prosecution, and make sure your workstation doesn't display the name of the last logged on user. These are things that won't keep any serious hacker out of your network, but will cover your legal backside and at least slow them down. Also, make sure that any modems connected to computers on your network are set to dial out only if they absolutely must be implemented. All an attacker needs is a wardialer and a modem set to auto-answer to bypass all the hard work you place in your firewall. If one machine becomes compromised, your entire network will become compromised as well. Limit modems as much as possible.

Viruses are increasing in popularity and ease of manufacture at a break-neck pace. According to Network Associates, there are more than 57,000 viruses in existence , and ICSA.NET states that 99.67% of companies surveyed had at least one virus encounter in the year 2000, while 51% said they had at least on "virus disaster" during the last 12-month period . They also tell us that the number of corporations infected has grown by 20% in the last year alone. While many of these viruses are aimed at Microsoft operating systems and products, no system is secure out of the box, and desktop virus scanning tools are a necessity in any network administrator's kit. Installing and setting up a regular schedule for updating your virus definition files is a mandatory function.

It will save you much valuable time to spend a few hours researching the various vendors before implementation. Different vendors offer different features. One of great concern to the small IT department is going to be method through which the software is loaded onto the clients. Perhaps the simplest manner is to purchase a CD-ROM with the software installation files on it and visit each workstation individually. This is quite time consumptive, though. Another method would be to place an image of the software on a network share and instruct users to download and install it themselves. This is more time effective, but obviously leaves you vulnerable to the diligence of already over worked end users to implement and update. Many vendors now offer a remote management application that will allow you to make logon scripts and transparently install the software upon the user's logon to the network. These consoles will also allow you to remotely monitor workstation infections as well as push updates out automagically. This can be a big time saver for the small group of technicians. Visit http://www.icsa.net/html/communities/antivirus/certification/certified_products/index.shtmlfor a list of ICSA certified anti-virus programs.

Even with the best anti-virus software, firewalls and password policies one thing is certain. Computers will crash. Just about every system admin has a midnight story of fatal exceptions, kernel panics or hard-drives grinding to a halt that required them to spend hours rebuilding a system. Of the millions of stories, the one constant in just about

every tale will be the restoration from backup. **Backup** is the big rock that is often overlooked until you need it, but then it is too late and you may as well get your interview suit pressed.

While it is possible to manually backup your critical data every day, to save time and ensure consistency it is best left to an automated process. This can be accomplished without extra cost using tar, dump & dd (or cpio for certain systems) on *NIX machines, and can be scheduled using the NTBackup program in Windows NT/2000. There are also several third party utilities that enhance the functionality and scalability of the backup process for most operating systems. Depending on your needs, one of these may be required.

Backups come in three types. Full, differential and incremental. A full backup backs up everything specified in the job, regardless of whether or not it has changed since the last backup. A differential backs up everything that has changed since the last full backup. An incremental backup backs up anything that has changed since the last full or incremental backup.

If you have the time to spare, performing a full backup every day would be best from a management point of view. That way, when your system crashes all you do is reload from a single tape. However, the amount of data may require more than the system's slow time, in which case it is best to do partial backups combined with a weekly full backup. Using Full and incremental backups is the most time efficient for backing up, but is least efficient to restore from. When the system goes down you must restore from the last full backup and then each incremental backup thereafter. If you use a differential backup, the restore process requires restoring the last full backup and the most recent differential backup. This will speed the restore considerably. A sample backup routine may include a full backup on the weekend and, depending on the amount of time it takes to complete the procedure, differential or incremental backups Monday-Thursday. Always store backup media in a locked environment with strict control of accessibility. It is also a good idea to store a regular copy of a full backup (such as a month end backup) off site in case of catastrophic disaster. Often backed up access control lists are not encrypted on backup media and therefore an easy target for attackers with access to the room.

Some high-availability networks are doing full backups daily with partial backups every hour, and other methods using partition snapshots on large-capacity disk arrays are able to back up any time with no system performance hit. But I digress...I'll wrap up this discussion on backing up your data by saying that it is one of the most unsung duties of the IT department, but you better be doing it regularly. Backup will save your backside eventually.

Checklists/documentation

Another often overlooked task in any IT department, much less the small department is **documentation**. In a world changing as quickly as IT, it usually seems that to take a

couple minutes and dedicate them to documentation is a waste of time. However, the amount of time it saves in the long run is exponential. Making use of a small database program such as Microsoft Access or Sun's Adabas is a simple and effective way to keep track of hardware and software configurations, PC locations, warranty and purchase order information. Keeping your wiring and network infrastructure documentation up to date will assist in troubleshooting and preparing for upgrades.

Checklists are another one of the things we always say we should do and never find time to accomplish. How many times do you say to yourself "I should document this right now, before I forget it," or "I wish I had time to write this down for next time?" Checklists are the investment we make today that pays off tomorrow. Not only are they ensuring consistency in tasks such as system implementation and software installation, they minimize the amount of guesswork needed for less-than-routine tasks. They also assist in the training of new personnel or even your replacement when you move on to bigger and better networks.

Small applications or scripts that create a routine for tedious tasks can also be of great service. An example is a Visual Basic program written for me by my predecessor to assist in the creation of users after he left the company. A seemingly simple task, user creation in the network I am primarily responsible for is a lengthy process, requiring creation and addition of each user in numerous modules of a poorly integrated application. The simple program prompts for the new user's name and a unique identifying number. It then generates a random password, lists all necessary group associations and permission levels and prints out a checklist to follow to ensure consistent creation and implementation. All I do is follow the checklist and shred the piece of paper when I'm done.

Basic Auditing

So once you have set up your network to be as secure as you can make it, how do you know if you are successful? Of course it's easy to tell when we are not successful by the information we lose or the destruction or defacement of our resources. But how do you know when someone is setting up for an attack, or about to use your network as a springboard to launch a bigger attack? Eric Cole, in his presentation at the Minneapolis Security Essential course said, "Prevention is ideal. Detection is a must." The way to detect malicious use of your network is through auditing.

There are a large number of software suites that will audit and monitor your network, ranging in price from free to several thousands of dollars. Going under the assumption that the small IT department usually comes with a small IT budget, I will limit this discussion to solutions that can be implemented for little or no money. Granted, you will often need to do more manual labor to get the info you need, but a firm grasp of the basics is going to give a firm understanding of the techniques and foundation from which to begin working.

But where to begin? There is so much information available it is difficult to know and feel confident that you are being thorough and prudent. Begin at the beginning and make sure your systems are collecting log data. In Windows NT you will enable auditing by opening Start > Programs > Administrative Tools > User Manager for Domains > Policies > Audit. Here you will find a check box that allows you to enable auditing, and several other checkboxes that allow you to specify what events you would like to audit. These audit messages are readable by using the event viewer, which can be reached by selecting Start > Programs > Administrative Tools > Event Viewer. You can then select either the system, security or application logs for specific messages relating to those facilities.

Unix and Linux do most of their logging automatically as long as certain files exist. These are /var/run/utmp, /var/log/wtmp and /var/log/btmp. They provide data on current logins, login history and bad logins. These are binary files and read using utilities such as "who, last and lastb" to name a few. Of note also are /var/log/messages for messages from the syslog and /var/log/secure for authentication. These files are text files and can be read with any text editor. They also have limited access, and you must have root privilege to read them. This is to prevent a casual attacker from erasing their tracks should they compromise the system and not gain root access.

When deciding what to monitor it is important to first "Know Thy System" and what is normal. If you don't know what it looks like in the first place, how can you tell if something is out of the ordinary. If possible, create a baseline from a freshly installed and secured machine. This is the best way to be sure you are checking a completely clean installation. You should know the answers to these questions:

-What services are running on which ports?
-Who has access to this system and from where?
-Where are your critical resources stored, and who should be able to access them?
-Who should be able to make changes to the system?
-Who has been given administrative privilege?

With these questions in mind, you can begin monitoring your logfiles. Always monitor failed logon attempts. A number of these in a short period of time, repeated failures or multiple users failing often would indicate that your system is under attack. This information can be gained by looking in Windows Event Viewer under the Security log or by executing a "lastb" command in a UNIX environment (remember to be sure that btmp has been created or this info won't be recorded). Along the same line, be sure to monitor successful logons (in the same place in Windows, by using "last" in UNIX) or you may not know when an attacker has become successful.

Two other major things to keep an eye on would be the accessing of sensitive data and alterations made to the permissions on your systems. You will want to know when users are trying to gain access to certain files, and to what extent they are successful. You also will want to look for times when a user will change permissions on a file or folder. If you notice that permissions have changed on the directory holding your HR payroll

information and the receptionist is now making more than the President of the company, you may have a problem. In Windows these can be monitored through the Event Viewer also, and Tripwire (http://www.tripwire.com) is a wonderful tool that monitors changes made to the system and alerts the administrator or designated user. There are versions for *NIX and Windows NT/2000.

It is also important to know what services are running on what ports on each of your systems. If you would like more information on ports, I suggest reading "An Explanation of Ports" by Arthur Hunt on the SANS website . A quick explanation is that a port is the part of TCP or UDP that allows services to connect. For instance, telnet waits (or "listens") for connections from other computers on port 23, ftp listens on port 21, etc. Each service will have a port that it listens on. You should know what ports are open on your system to know when a rogue service or application is available for connections without your knowledge. For instance, the Back Orifice trojan listens on ports 12345 or 31337. If you scan your system and find that one of these ports is open, you may have a problem.

Limiting the services running on each computer is a fundamental host perimeter protection method. For instance, does a workstation need to be running as a webserver? Do you need to be offering FTP services on each client of your network? Implementing the "Principle of Least Privilege" is a good rule of thumb. Turn off or eliminate all services that are not necessary to perform the job function. There are a number of software applications available for protecting individual computers, such as Zone Alarm (http://www.zonelabs.com) or BlackIce Defender (http://www.networkice.com) for Windows systems, while Bastille Linux (http://www.bastille-linux.org) supplies PERL scripts used to harden Red Hat and Mandrake Linux systems.

Port scanners can then be used to test your system. One of the best is Nmap, which along with port scanning will do other neat things like ping sweeps to monitor which IP addresses are connected to your network, remote operating system detection and a raft of other fun things to do with IP. The original Nmap runs only on Linux and can be downloaded for free at http://www.insecure.org, while nmapNT is a port for NT systems and can be downloaded freely at http://www.eeye.com/html/Research/Tools/nmapNT.html. The NT version has a few limitations because of the NDIS driver, but for the most part it is a good tool as well. A simple way to automate the utilization of this tool would be to run it as part of a script and then schedule it to run as part of a cron job or using the AT command in NT. Dump the output to a text file that can be scanned (either manually or with a tool such as a PERL script) for known vulnerabilities or services that are out of the ordinary.

While monitoring doesn't prevent a security breach, it will let you know about a compromise. This gives you the opportunity to catch the hacker as well as re-secure your systems. It is a good idea to run these tools from a remote host on your network from a CD burned expressly for the purpose of security scanning. That way you know that the tools you are using to check your network are free from hacker modification. It is also a

good idea to regularly back up and archive your logs for later examination should you find a security breach.

Getting the most info in the least amount of time

Many times lone administrators find themselves feeling somewhat like an island in the midst of a sea filled with savvy attackers and vicious worms and viruses. Often times it seems as though we are fighting a losing battle and the hackers are winning if only because they out number us so greatly. This is why it is so important to get to know other professionals in the industry and maintain contact with them. A common forum of security-minded professionals is a must for the small IT department.

Users groups are an excellent tool to use for many reasons. Chances are you can find a group that caters to your particular operating system, network infrastructure, applications and just about everything a geek would ever want to discuss. You can find them by an internet search or try a local bookstore for ads in computing magazines. You also might find other geeks on IRC or ICQ. If you look hard enough, you will find them. There are also lists of newsgroups that can be emailed for assistance. You can find a list at http://groups.google.com. There will be a great number of lists, and selecting the link marked "comp" will bring you to a list of computer related topics. This is a smorgasbord of topics, and you will need to do some digging to find the information you want. I often find that while searching for help with a particular issue I'll uncover loads of information that is useful. It may not always be about the topic I began looking for, but helpful nonetheless.

Other resources that prove invaluable are **mailing lists** geared toward security professionals. In a single email you can read about the latest attacks and viruses plaguing administrators worldwide. This is the internet as it was intended to be, with people sharing information freely to better the community as a whole. It is also a good idea to find a few different websites that you like that post up to date info on information security. Of course, there are probably thousands of sites, and it may take some time to find a source of info that you enjoy and find useful. It is again worth the research time to find out who is offering their insight and what their qualifications are. Some great sites and lists that have reliable information are:

For a list of the top ten internet threats try the SANS top ten list
http://www.sans.org/topten.htm
For quality, up to date info in a customizable email newsletter try SANS security digests at http://www.sans.org/sansnews
CERT mailing lists are invaluable for near real time alerts and a wealth of online knowledge at http://www.cert.org/
Bugtraq mailing lists are operating system specific and can be subscribed to at http://www.securityfocus.com/
A good all-around site for security information is http://www.securityportal.com/

Again, there are countless sites and many may have fantastic information. You will most likely want to check out the website of your antivirus software vendor for mailing lists and quick info on virus threats. Take some time to research and dig and you will never have to feel like the only good guy in a sea of bad guys.

Outsourcing

Because of the level of knowledge required to ensure a secure environment, the aspect of bringing in quality assistance from an outside vendor is not only appealing but necessary in some cases. It is just seemingly impossible to know everything about everything and do an adequate job on them all. Before hiring a consultant or contractor some research is required, and care should be taken to retain an experienced, knowledgeable and responsive individual or company for the project. Checking the Better Business Bureau and your prospective consultant's references are also a wise time investment.

Deciding what to outsource is a prime concern, especially where information security is concerned. Will you outsource certain functions in your infrastructure, such as firewalls, databases or hardware support? Will you outsource implementation only or include maintenance of the product or service? What will the level of service be, and will that include training of you or someone on your staff to handle day-to-day maintenance?

Regardless of the service or product you decide to utilize outside people on, defining the requirements, expectations and metrics will help ensure a successful outsourcing partnership. In other words, it is imperative that everyone know what the expectations of the project are and how those expectations are going to be measured. How does your partner share the risk, and how do you handle non-compliance? Often times levying fines for unsatisfactory work gets the attention of consultants, and it is best to have established a clear avenue for complaint resolution that includes those in upper management. Also, it may be wise to have a clause entered in the contract that the personnel initially assigned to a project will remain on it until completion (or at least for a specific amount of time). This safeguards you from companies bringing in their "top-guns" to secure your business and handing it off to junior staff members to save money. In some cases it may be wise to establish a committee to meet regularly for the purpose of monitoring and reporting on compliance of the contract. As with everything, documentation is essential. Having a sound legal contract with defined goals and metrics will save much time and money while avoiding the process of "due diligence" in conflict resolution.

Conclusion

There are many problems facing the security community in general, and many times these seem amplified to the small IT department. . Take the time to learn the basics and focus on them so that you have a solid foundation to work from, and then examine your situation more closely to refine your approach. Add automation in areas that are time-consuming, tedious and error-prone, and before long your process and procedure will be

running smooth. With some research and diligence, a secure information system is not only possible but achievable and realistic, no matter how small your department is.

Resources/Footnotes

1) Crabb-Guel, Michelle "Model Security Policies"
http://www.sans.org/newlook/resources/policies/policies.htm

2) "Password Management Best Practices" M-Tech
http://www.psynch.com/docs/best_practices.pdf March 2001
3) Jones, Deri "The Top 10 Security Holes in 'Real World' Practise" 2001
http://www.nta-monitor.com/news/top-10.htm

4) Network Associates "Virus Information Library" http://vil.nai.com/vil/default.asp

5) Bridwell, Lawrence and Trippett, Peter "ICSA Labs 6th Annual Computer Virus Prevalence Survey 2000" download PDF at
http://www.trusecure.com/html/tspub/index.shtml

6) Hunt, Arthur "An Explanation of Ports"
http://www.sans.org/infosecFAQ/securitybasics/ports.htm

Veal III, Ruffin. "Private Lessons for the Public Sector" June 15, 2001.
http://www.cio.com/archive/051501/re.html

Tardugno, Tony. "Keys to Successful Outsourcing" June 29, 2001.
http://www.informit.com/content/index.asp?product_id={DEAA8F07-5CD9-4FF2-8F7A-F805CBBF8865}&news=true