Global Information Assurance Certification Paper

The Computer Security Threat to Small and Medium Sized Businesses – A Manager's Primer

Michael A. Regan

16 August 2001

Table of Contents

Chapter 1

Introduction

The business use of computers has evolved with the widespread introduction of high speed data access at relatively low cost. This evolution allows many companies that formerly used computers as stand alone word processors or for database storage to network the computers and attach that network to the Internet. While this concept provides many benefits to the company including telecommuting and support to a mobile sales force, it also brings with it the potential for the introduction of computer viruses and hacking. This paper seeks to provide non-technical, easily understood, information for the business executive seeking to capitalize on the benefits provided by Internet access while at the same time protecting his internal network from viruses and hackers.

On a regular basis, the news contains reports of the latest computer virus, worm or the exploits of hackers. This type of information could lead an executive to the conclusion that the threat does not justify the benefits derived by using the Internet for daily business transactions. While the threats are very real, they can be dealt with once they are understood.

The advent of Digital Subscriber Loop (DSL) and Cable modem provide opportunities for many small and medium sized businesses to access the Internet. This access may have several benefits such as providing a web site for customer access, providing a corporate email system and a mechanism for the transfer of large files. High speed continuous Internet access which may have been previously relegated to large corporations is know widely and economically available.

This large scale availability of access provides those intent on creating mischief fertile ground. In order to protect company access to the Internet and the integrity of company data, steps must be taken to ensure the security of the company's data and network. Do not be lulled into a false sense of security by thinking that if you only use dial up modems, rather than continuous high speed Internet access, that you will be safe from attack. Many attackers look at modems as a back door into a network that might be attached to the Internet and protected by sophisticated firewalls and intrusion detection systems.

The Systems Administration, Networking and Security Institute (SANS) along with many other security organizations consider a three pronged approach to computer security. This approach covers the Confidentiality, Integrity and Availability of computer data to ensure that the data is kept from compromise and is available when required. We will discuss each of these elements in the following paragraphs.

"Confidentiality refers to the areas affecting the need to keep information private or secret and to prevent disclosure of information to those who do not need to use it."[1] Confidentiality of both company and customer data is critical in an age of e-commerce.

In the chapters that follow, you will see how the confidentiality of company data can be maintained while at the same time allowing Internet access.

"Integrity is the notion that information should be complete and unaltered as it is used and that changes are made only by authorized people and properly recorded."[2] The integrity of data held in company databases must be maintained so that those who use this data for making business decisions can do so with confidence. Mechanisms must be in place to prevent unauthorized changes from being made to company databases. Consider the business impact of someone making unauthorized entries into a delivery system database that results in the delivery of a large amount of product that was never invoiced and the loss of revenue that might result from such actions.

"Availability refers to the need to have information available for use when it is needed and in a form that is usable"[3] Much has been written in the press concerning "Denial of Service" attacks which are directed at company's web sites in order to make the site unavailable. While this is the most widely publicized method of making data or sites unavailable it is not the only attack. A hacker may attack a company's network in order to crash the server and bring the network to a halt. Installing gateways or firewalls can protect your internal network from outside attack and preserve the availability of your network and database.

This paper will further define the mechanisms for ensuring this Confidentiality, Integrity and Availability in the chapters that follow this Introduction. When reading this paper, keep in mind the elements of Confidentiality, Integrity and Availability and you will have a better appreciation for how your network and data can be secured.

The company that uses the Internet or provides remote access to its internal network must also provide for protection of that network and associated data. One of the first steps in security your network and data is the creation of a company computer security policy. The company security policy must be established to set the framework for how the company will secure its computers and information. This policy must be easily understood and supported by both management and personnel. The policy should address threats posed by email, outside attackers while at the same time defining the acceptable uses of the network and company data by employees. The company email system must be protected by anti-virus software to preclude the introduction of a computer virus on company computers. Gateways or firewalls must be installed to control access to and from the Internet. Intrusion Detection systems must be installed, and properly configured, to prevent the hacker from unauthorized entry or if entry is made then appropriate alerts are sounded. All of this sounds like a formidable task for the small and medium sized business, however, can a business not afford protecting sensitive company data?

"Why should we make an investment to protect our data, we do daily backups and can quickly restore operations?" That question is often asked by businesses who view that they have little to lose if they are attacked and their network or database compromised. It does not take much "crystal ball gazing" to see how companies that fail to protect

their network from intrusion or customer data from compromise might find themselves subject to lawsuits for damages should attackers gain access to personal information such as credit card numbers that we later used for criminal purposes. Also, an attacker could break in to your network and take over a computer system from which a denial of service attack could be launched against another party. These types of attacks have previously been launched against a target using a large number of compromised computer systems without the owner even being aware that their systems were used for such purposes. Failure to exercise due care and protect your computers and the data they contain might be used as the basis for a law suit against your company by the victims of a denial of service attack or identity theft victim.

"Our Internet access, E-commerce and Email is provided by a vendor, why do I need to be concerned about computer security?" In an era of outsourcing, many companies lose sight of what their vendor is doing and how they might be protecting, or not protecting, the company's data. Managers should be familiar with the concepts shown in this paper to ensure that their vendors are properly protecting company data. Knowing the concepts and basics helps you formulate the right questions to ask your vendor.

As we move forward in this paper, we will address computer security by focusing on providing for the confidentiality of data, ensuring the integrity of that data and providing mechanisms which will make data available when it is required. When reading this paper do not come to the mistaken conclusion that Internet access is more trouble than it is worth. All of the threats that are identified can be reduced or eliminated by developing an understanding of the threat and the appropriate safeguards.

While reading this paper do not come to the mistaken conclusion that Internet access and providing remote access to your network is more trouble than it is worth. All of the threats we identify can be reduced or eliminated by developing an understanding of the threat and the appropriate safeguards. No business endeavor is without risk. By understanding the risks and employing the necessary safeguards, it possible to use the Internet as a business tool. The chapter on standardization looks at what the future may hold concerning international standards for protection of information and the reasons to be concerned about computer security now.

End Notes:

[1] Systems Administration, Networking and Security Institute (SANS), "Information Security Kickstart Highlights", Basic Security Management, pg 1-19.

[2] Ibid

[3] Ibid

Chapter 2

ENVIRONMENT

"Some of the main reasons for establishing networks in small businesses include file and print sharing; remote access by employees and customers and providing internet access to workers." [4] Small businesses with network operating systems will most likely have access to the internet using some of the access methods described in the next paragraph. These same companies are unlikely to have fulltime dedicated automation personnel due to the high salaries these types of personnel normally receive. This often results in operating systems being installed that are not optimized for security and not continuously updated with the latest software patches.

The declining cost and rapid spread of high speed internet service is making rapid inroads into the small and medium sized business segments of the market. With increased emphasis on telecommuting and home based small offices, internet access will become ever more critical to daily business operations in the future. The major growth, in business high speed internet access, will be in cable modem access to small businesses and home based small offices which jointly number about 11,281,000 locations. In addition to small businesses and home based small offices, many of the medium sized companies have established remote branch offices that require high speed internet access to communicate with the main office. In a survey conducted by Cahners In-Stat Group of 322 businesses the following type of high speed access were in use:

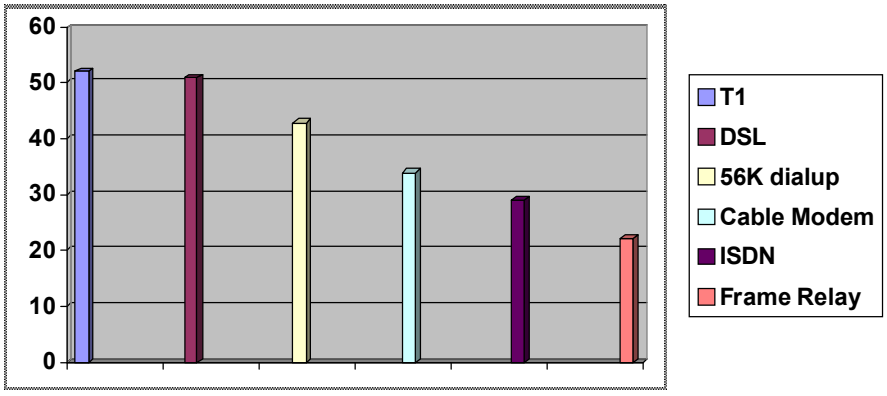

Figure 2, Current Broadband Business Use [5]

As you can see from the previous graph, DSL and Cable Modem make up a large percentage of the internet access methods used by businesses participating in this survey. The rapid spread of these methods of internet access will only continue to soar in the coming years.

The nature of broadband service is such that DSL and Cable Modem provide “always on” access to and from wide area networks which increases the potential for compromise of company information. This potential for compromise is increased by the very fact that hackers now have more opportunity to attack this stationary target. Many Internet Service Providers (ISP) who support DSL and Cable Modem provide static Internet Protocol (IP) addresses which serve as the mailing address for the internet. These static IP addresses allow a hacker to continue to locate the target company on the internet and subject that network node to various attacks meant to break into that computer system. Some ISP's provide "rotating" IP addresses which might not always be assigned to the same network node. This system of "rotational addresses" provide only marginally greater security than ISP's which use IP addresses. Companies who use a dial-up method of accessing the internet have a somewhat more secure means of internet access since their vulnerability is only while their system is connected to the internet over the telephone. Also, most ISP's assign IP addresses only for that connection and once the connection is broken that particular address is available for assignment to the next caller. The dangers posed by the modem will be covered in another chapter.

The increasing use of the Internet by the small and medium sized business segments results in a growing need for managers to learn more about computer security which is the purpose of this paper. In order to make proper business decisions, the manager must also know about the threat to their computer data and networks.

End Notes:

4. Microsoft, Small Business Server, Partner’s Guide

5. Cahner’s In-Stat Group, “Moving Towards Broadband Ubiquity in U.S. Business Markets”, Apr 2001, pg 19.

Chapter 3

Threat

As mentioned previously, the SANS Institute breaks down computer security into three basic elements of Confidentiality, Integrity and Availability. To have a secure computer system, each of the three elements must be considered when designing and installing computer network in order to have a secure system. Attacks against computer systems will normally involved compromising at least one, if not more, of these elements. In this chapter, we will explain the purpose of an attack, types of attackers, phases of an attack, and the various types of attacks that a perpetrated against a computer system.

The purpose of a computer attack is to takeover a targeted computer or to attack a computer in such a manner as to cause the operating system to crash or become unavailable to outside users. While some attackers are criminals attempting to gain access to lists of customers and associated credit card numbers, still others are attempting to access sensitive corporate data which might be of use to your competition. The advent of automated scripts allows many novice hackers to conduct sophisticated attacks without detailed knowledge of the inner workings of telecommunications software. These types of novice attackers can be likened to hobbyists and derive satisfaction out of finding unprotected systems to attack in order to gain control of the system or defeating systems with minimum types of protection.

Types of Attackers: Mr. Daniel Tatone, author of "Network Security: What are you waiting for?" defines hackers as follows:

> "There are principally three types of attackers: The first… is the Amateur Hacker also knows as a "cracker". Crackers have developed an underground community often comprised of young individuals in their teens known as "Script Kiddies". These Script Kiddies pride themselves on their web defacements, denial of service attacks (as seen against Yahoo and eBay in January 2000) and system breaches. They usually do not understand the technical details behind the attacks that they perform; they rather collect and rely on already made hacker tools and scripts to perform their system breaches. They usually sign their "Hacker Alias" or "Hacker Group" on the website they deface, greet their fellow hackers, dismiss their "rivals" in the hacker community and occasionally post a political message…The second type of hacker is the Professional Hacker. These are individuals who are often paid to perform corporate espionage and the likes to gain sensitive corporate information from companies for their competitors. These Hackers enjoy the challenge of the hack and are extremely meticulous in covering their tracks. Their technical abilities are second to none, they understand the details and inner workings of networking and information systems, and are masterminds at social engineering. Unlike the crackers, they do no flaunt their deeds, and are virtually unknown in the underground community… The third type of hacker is the disgruntled employee

or the disgruntled ex-employee, who through his/her technical know how and internal access to the information systems of the corporate network can wreak havoc on the information systems infrastructure." [6]

Phases of attacks: There are three phases to a computer attack shown as follows:

- First, the attacker must map the target computer system. This is done to identify the target by gaining information on the internet address of the target, type of operating system running on the target and any open access points (know as ports) on the target. The target computer may be one directly connected to the internet via cable modem, DSL, or other high speed data communications circuits or one that has a modem installed. Scanning programs exist which allow an attacker to specify a range of internet addresses, or telephone numbers in the case of modems, and the scanner will attempt to locate addresses or phone numbers that have a system attached.

- The second phase involves conducting reconnaissance against the target to determine if information can be developed which will make the attacker's effort easier to accomplish. This phase of the attack involves hunting for user account names and passwords. While at first look this may seem to be an easily defended against attack, it is in reality more difficult. The attacker often uses a concept known as "social engineering" where the attacker calls the targeted business and masquerades as someone from the help desk, or your Internet Service Provider, and then asks the user for their user account name and password. Once that information is gathered, the attacker will then attempt to logon to the system and masquerade as a legitimate user. Another technique used by the attacker is known as "dumpster diving" where the attacker rummages through the trash of a target looking for lists of employees names. These names can then be used as ammunition for the attack via remote access. Sometimes this second phase will result in access to the target system without having to resort to the third phase.

- The third phase involves attempting to gain access to the target System without previous knowledge of a valid user id and password. Depending on the software installed, there may be other methods of gaining entry into a system without using a user id and password to logon. This third phase requires more skill on the part of the attacker. Should the second phase be unsuccessful, the attacker may move on to this third phase. In this phase, the attacker must find a vulnerability on the target that can be used to compromise and gain unauthorized access to the system. Operating system software installed without forethought being given to security can leave a computer system with a default installation that has not been hardened to reduce the possibility of unauthorized access which could result in vulnerabilities which can be exploited by the attacker during this phase of the attack. Once the attacker has access to the target system, he may be free to roam about the network looking for information of interest, planting Trojan Horse programs, modifying or deleting data all without your knowledge. At this point the Integrity of the target computer system has been compromised.

Types of attacks: Computers are vulnerable to a number of different types of attacks. These attacks can be broken down into several different categories:

- Viruses and worms: The virus is normally introduced into the target system by either an email attachment or loaded from previously infected software, which then infects the computer on which the software is loaded. Recently, Symantec reported that the total number of viruses known to exist in 1990 was 80, compared with 2001 when 50,000 viruses were know to exist.[7] A detailed discussion of viruses and worms is beyond the scope of this paper. Additional information on viruses and worms and the differences between them can be found at the Symantec Antivirus Research Center website at http://www.sarc.com/avcenter/reference/worm.vs.virus.pdf.

- Password Attacks: This type of attack involves attempting to break into a system by continuous attempts to logon using various passwords. Hacker use a program that will use all variations of letters, numbers and special characters in an attempt to find a valid password. Depending on the complexity of passwords used, the longer the attack will take to succeed and the more likely it will be identified during a review of security system logs. For this reason, your password policy should require "strong passwords" which are at least eight characters long and composed of lower case, upper case, numbers and special characters.

- Trojan Horse: Software which has been implanted on a target system which allows unauthorized access to that system circumventing the normal access controls that are in place. The Trojan program can be introduced into the target system by accessing a web site that contains the Trojan, opening an email attachment that contains a Trojan, using software that implants the Trojan while performing some legitimate action, or by an attacker gaining unauthorized access to your system. Naturally, the user in unaware of what is happening while the Trojan is being installed. These Trojan programs can allow a hacker to take control of the target system and then have that system attack another system. A Trojan used in this manner can perform denial of service attacks on a third system where the third system is unable to function due receiving a large number of requests effectively denying access to that third system for legitimate requests. A Trojan can also be used to capture data on the target system and send that data to an attackers computer. This data could be passwords, credit card numbers or other sensitive data.

- Denial of Service Attacks: Web servers operate on a connection basis

where a system requests a connection and the web server responds to that connection. There are a finite number of connections that a web server can service at one time. The Denial of Service attack attempts to have a large number of systems simultaneously request connections with a specific web server in an attempt to exceed the number of connections that the web server can handle. These connections are never fully completed so the web server waits for a period of time before terminating the connection thus using up connections which would otherwise be used by a

customer. The attacker uses other systems he has compromised and on which he has loaded a Trojan which will conduct the attack. These compromised systems are referred to as "zombies" and if the attack is traced back it will be traced to the compromised systems rather than that of the hacker. The Denial of Service attack compromises the Availability of the target computer system.

- Communications Intercept Attacks: The interception of data communications while not a prevalent as other forms of attack, is possible for the professional attacker, and is an example of a compromise of confidentiality. The introduction of wireless computer networks that avoid the necessity of installing network cable are particularly prone to this type of attack. These types of sophisticated attacks are beyond the scope of this paper.

Methods of access to a target computer system:

- Remote Access over Modem: The attacker using this type of attack can make use of a program called a "war dialer". The war dialer calls every telephone number in a specified range of numbers looking for an answer by a modem. These programs are intelligent enough to differentiate between the tones of a facsimile machine and that of a modem. When a modem is located, that number is flagged for later review by the hacker. A war dialer provides a tool for the hacker to locate computer systems that might not be tied directly to the internet.

- Remote Access over the Internet: Once the reconnaissance of the target system is complete, the attacker can possibly determine what type of operating system is being used on the target. Based on that determination, the attacker can look up that operating system on various hacker web sites that will list the known vulnerabilities of the target (this also applies to targets located by a war dialer) and then figure out how to exploit that system's vulnerabilities. The attacker may be lucky enough to find a system whose vulnerabilities have not been fixed by updates and patches provided by the manufacturer. The attacker can then exploit that vulnerability and may be able to gain entry into the system. Another option for the attacker, should they be unable to gain entry into the system, could be to attack the target in such a manner as to bring down the operating system.

Hoaxes: Symantec has identified over 125 hoaxes which regularly circulate around the Internet along with a notice that you should send that email to everyone you know.[8] The intent of these hoaxes is to flood email systems with meaningless traffic about not existent viruses. This can have results similar to the Denial of Service attacks noted above.

End Notes:

6. Tatone, Daniel, Montreal Business Magazine, Mar 2001, "Network Security: What

are you waiting for?”
http://mooseland.montreal.qc.ca/images/article.jpg

7. TechTV reporting on Code Red Worm quoted Symantec virus data on 19 July 2001

8. Symantec, Symantec Security Update, Hoaxes
http://www.sarc.com/avcenter/hoax.html

Chapter 4

Safeguards

In order to properly protect you computer system requires that time be devoted for a critical examination of your system. This examination requires analyzing your system to identify vulnerabilities and then taking action to resolve those vulnerabilities. Once a system has been hardened against attack, continuous effort is required to ensure that the system remains hardened. Every week new software vulnerabilities are identified and software patches are created. Additionally, virus definition software requires routine updates to remain effective. The next few paragraphs will provide a blueprint for hardening your system to reduce the possibility of attack. While no one connected to a computer network, with or without internet or remote access, is immune from attack, action can be taken to significantly reduce your vulnerabilities and identify when your system might be under attack.

Step 1, The System Map: The first step is to identify how your computer system is setup. This step is required for both internal networks (intranets) and single systems attached to the Internet along with any intranets that are not attached to the Internet but provide remote access. The following must be taken into account when creating the system map:

- Which computers are connected to your internal network?

- What types of software and operating systems are running on those computers? What is the current version of the software? Are the appropriate software updates installed?

- Which systems are directly connected to the Internet? Are these same systems connected to your internal network?

- Which systems have modems installed? Are the modems set for auto answer?

- What type of virus scanning software is installed and on which systems? Are procedures in place to update the virus data files?

- What type of intrusion detection system is installed? Are the logs reviewed on a regular and frequent basis?

- What are your critical business applications and data?

Step 2, Develop a Computer Security Policy: This step involves defining the company policy for a variety of issues related to use of computers by company employees and how security will be implemented. The policy must be easily understood, widely distributed and readily available for the company's employees.

The following issues must be considered when creating the company computer security policy:

- What are the authorized uses for company computers?

- What sort of password policy will be used including length of passwords, composition of passwords (i.e. must contain numbers, upper case, lower case and special characters) and frequency for changing passwords?

- Who is responsible for updating the Antivirus software and how often that person will check for updates? What action will be taken if a virus strikes?

- Who is responsible for reviewing the Intrusion Detection System logs, how often the logs will be reviewed and what action will be taken if intrusion attempts are detected?

There may be a need to have two policies, one widely distributed to all employees and a second, more detailed policy for use by management and the automation staff. The second policy would provide a copy of the system map, step by step checklists for dealing with viruses and intrusions. This second policy requires safeguarding to prevent unauthorized persons from having access to it. This type of document would, if lost, provide an attacker with a blueprint of your system and the defenses you have in place.

Step 3, Harden the Software: This is done by taking a critical look at what Software is installed on the system and if the software has the current updates and patches installed. Check out the software manufacturers web site to determine if there are updates and patches which should be installed. Often systems are compromised by hackers when a software update or patch was available that could have prevented the hacker from gaining access to your system via that particular software program. Also, remove any sample system or program data from your production system as some of this sample data might pose a security hole on your system. This is particularly true if you are using Microsoft Internet Information Server (IIS) which has sample program scripts which are easily compromised by hackers. Once these sample scripts are removed this program is much more secure. "Common Gateway Interface (CGI) is the language that programmers use to display and read input to a WWW based form. The examples furnished with WWW server programs and not written with security in mind. Hackers have discovered that they can subvert these programs and cause them to run other programs. You should remove all of these examples from your production WWW server. There's no need for them to be on the production system."[9] While CGI scripts can be exploited to gain access to a web server with the intent of changing or defacing the content of web pages, a more sinister outcome would be to plant a Trojan program that could be activated at a later time to launch distributed attacks or denial of service attacks. SANS further identified

problems with the Microsoft Internet Information Server (IIS), "Windows NT and Windows 2000 Web servers use IIS to support web services. The IIS program has a component called Remote Data Services (RDS) that could allow a hacker to run remote commands with administrator privileges. Some of IIS' components are vulnerable to a buffer overflow type attack which lets the hacker gain full control of the system. Since the hacker can run remote commands on a compromised server, you can imagine the types of abuse that can happen. Obvious things include modifying the www pages(s), disabling the server, and launching an attack on a site. More subtle things include adding userids on the server, modifying Active Directory components and installing keystroke records on the server system."[10]
Enable logging and auditing on servers and gateways in order to record attempts at accessing databases, invalid logon attempts and other events will provide useful information and early warning should someone attempt unauthorized access to your network or database. This logging helps ensure that the integrity of your system is maintained.

Step 4, Reduce the number of access points and secure the remaining access points: This step requires a review of the system map to identify which systems have access directly to the internet or remote access outside the network. The goal is to reduce the number of access points to the minimum required and then install software to monitor the flow of data into and out of your network.

Step 5, Look for hidden entrance points: There may be systems on your network that have modems installed which would allow uncontrolled access into your network. The "war dialer" software, mentioned previously, can be setup to dial all the phone numbers in your company looking for modems that are setup for auto answer. The war dialer data can then be used to locate these hidden access points. The war dialer program will not identify modems which are used for dial out only which could be identified by a quick physical inspection of each computer. To avoid unauthorized and uncontrolled external access these modems should be removed which will reduce the possibility of an employee accessing their personal email account, downloading a file infected with a virus and then infecting your network effectively bypassing your anti-virus software.

Step 6, Install a gateway or firewall to shield your internal network from the Internet. Reduce the number of open ports on the gateway or firewall to the minimum required for your network. Open ports on the gateway or firewall provide opportunities for an attacker to identify what type of operation system is in use on your network and enable the attacker to formulate a plan of attack. At this point a mini risk assessment must be conducted to determine the impact of having particular ports open versus what types of access to the Internet will be denied to users. Locking down certain ports may result in users being unable to use certain types of software functions. Once a decision is made to lock down a port, the users must be educated and if that access is required some sort of workaround must be established. Failure to educate users often results in users attempting to work around the firewall which often ends up opening even greater security holes. To get a perspective on how this can impact users, read

an article entitled “The Downside of Network Security”, by Mr. Jim Williams.[11] This article explains one person’s experience balancing computer security with operational requirements. One additional benefit derived by installing a firewall at your gateway to the Internet is the ability to control what websites are being accessed by employees. Sites that rob bandwidth from your network and do not contribute to your company’s production, like auction sites, pornography sites, sports sites and similar sites, can be place on restricted lists so that employees cannot access them from the internal network. Also, access to the web can be restricted to certain systems that have a valid need for this type of access.

Step 7, Install Intrusion Detection Software (IDS) which functions as the burglar alarm for your network. As with real burglar alarms, there is no such thing as a “false alarm”. Once the IDS is installed you can expect to see numerous attempts to scan your network by potential hackers. In addition to installing a firewall at the access point to the Internet, consider installing additional “personal firewall” software at each user’s computer and server. This will provide defense in depth so that in the event a hacker is able to bypass your gateway’s firewall, they will be detected should they attempt to break into systems located on your internal network. An ideal plan is to have one type of IDS on your gateway and a different type for the workstations and servers. This way should a particular type of attack by unrecognized by the IDS at the firewall, it may be detected by the IDS installed on the workstations and servers. One important function that should not be overlooked is a regular review of the logs generated by the IDS system. Early detection of attempts to scan your network by a potential attacker can be used to block that attackers address before they have time to mount a more in-depth attack. Several IDS systems allow for the logs to be sent to a central location making the review process easier to accomplish.

Step 8, Install Anti-virus software to detect infected email which contains a virus.

Numerous anti-virus software products exist which can be installed at the gateway and on individual workstations to detect the presence of a virus. As with IDS systems, it is important to update the virus definition files on a regular and frequent basis to ensure that your network has the most up to date protection possible. It is also necessary to check for software updates for the anti-virus software to again ensure the your system is adequately protected. One important step that is often overlooked is the need to educate the user on the need to be wary about opening email attachments that come from unknown addresses and the appropriate action to be taken when attachments are received. The Computer Security Policy referred to in Step 1, should provide easily understood guidance for the user on what to do if they believe that their system has been infected with a virus. While the guidance provided in this step may not provide total protection against all viruses, it does provide protection for many of the common viruses found on the Internet. Additional defense in depth can be obtained by having one vendors anti-virus software on the firewall or email server and another vendor’s product on the workstations.

Step 9, After all the previous steps have been completed a security audit should

be conducted to determine how well the overall security system is functioning. The audit could identify additional problems or vulnerabilities which need to be corrected. Once the system audit is completed, management may be required to perform a risk analysis to balance the needs for security versus the operational requirements of the business. In certain cases due to business requirements, a vulnerability may continue to exist and appropriate measures taken to mitigate the damage that can be inflicted along with plans to quickly respond to an attack that exploits that vulnerability. The results of the system audit should be kept on file, in a secure location, so as to have a baseline for future security audits.

Summary: You may be thinking that this is a very complex issue and that since you are a small or medium sized business, no one would want to attack you. "But from a Hacker's perspective it is easier to attack a small/medium size business who has mistakenly connected their backbone directly onto the Internet with no firewall or means of access control rather than a government agency or large firm (the "big boys" like Microsoft or Cisco) who have invested a large amount of resources in securing their infrastructure. Once a small/medium business has been compromised the attacker could then launch attacks anonymously against the "Big boys" from there."[12] While this may at first look seem to be a daunting task for the small and medium sized company, there are numerous computer security consultants which can assist the company in developing a good computer security system should this be beyond the capabilities of in house staff.

End Notes:

9. SANS Institute, Marchany, Randy and Craddock, Mary, "The Top 10 Internet Security Vulnerabilities – A Primer"
http://www.sans.org/audio/sanstop10presentation.pdf

10. Ibid

11. About.com, "The Downside of Network Security", Jim Williams,
http://netsecurity.about.com/library/weekly/aa122999b.htm

12. Tatone, Daniel, Montreal Business Magazine, Mar 2001, "Network Security: What are you waiting for"
http://mooseland.montreal.qc.ca/images/article.jpg

Chapter 5

International Standards for Information Security

The business world continues to move towards developing standards for various types of systems. The creation of the International Organization for Standardization (ISO) provided a body to coordinate the development of standards on a worldwide basis. One ISO standard that many companies are familiar with is the ISO 9000 standard for quality control and assurance. Businesses have grown accustomed to looking for ISO 9000 certification from their suppliers. The Internet has fostered new ways to coordinate business activities on a worldwide basis, which allows businesses to share personal data of their customers. The threats mentioned in previous sections of this paper create the very real possibility for loss or compromise of sensitive customer data such as names, social security numbers, dates of birth and credit card numbers. In order to protect this sensitive information the ISO has created a standard for information security.

In regards to protection of sensitive information, the British developed British Standard 7799 the "Code of Practice for Information Security Management" which has grown into the ISO standard 17799. Both the ISO and British standards take into account the three SANS security cornerstones of Confidentiality, Integrity and Availability. The BS 7799 standard [13] requires establishment of ten key controls:

- A documented information security policy
- Allocation of information security responsibilities within the organization
- Information security education and training
- Security incident reporting and response
- Virus detection and prevention controls
- Business continuity planning
- Control of proprietary software copying
- Critical record management processes
- Protection of personal data (privacy)
- Periodic compliance reviews

These ten controls cover more than just the electronic storage of data and extend to both physical and electronic storage. Data transmitted as facsimiles and via letter would also be covered under this standard.

The ISO 17799 standard has evolved from the British Standard and will be viewed in the future as the standard by which companies exchange and protect sensitive information. The need for this standard is shown in the results of a survey conducted by Gamma Secure Systems, Ltd. This survey of 1102 responses determined the following:

- 927 had internet access

- 881 were very dependent on their computer network (Network access is a portion of the SANS cornerstone for Availability.)

- 880 expressed concern about leakage of sensitive information to outsiders (Loss or compromise of information is a portion of the SANS cornerstone for Confidentiality.)

- 400 felt that their customers do care that information is reliable and that about 390 felt that they could spot and correct errors before their customers (The Integrity SANS cornerstone applies to this portion.)[14]

GAMMA has created a web site that a company can use to determine whether ISO 17799 is applicable to their organization.[15] While the questionnaire is written from the perspective of a supplier it can also be used by a customer to determine the level of ISO 17799 compliance that they should require from prospective suppliers.

In the future, information protection standards will be used for evaluating the business relationships of both customers and suppliers. The customer will evaluate suppliers based on the supplier having a system in place to protect sensitive customer information. The supplier will use the standard to ensure that both customer data and sensitive corporate data are protected from compromise. The savvy businessperson will enact ISO 17799 and advertise their compliance with that standard as part of their marketing process. The savvy customer will look for ISO 17799 compliance when selecting from a myriad of potential suppliers of goods and services to ensure that their sensitive information is appropriately protected. The commercial uses of the Internet to pass business information from one organization to another provide new opportunities for companies working in a global marketplace. These benefits far outweigh the risks posed by attackers, if a good strategy is in place to protect sensitive information. In addition, compliance with ISO 17799 may also provide some legal protection from lawsuits that might arise involving the loss of sensitive information in the event of a successful attack against a company network by demonstrating the use of “best practices” by the company involved.

End Notes:

13. Toward Standardization of Information Security: BS 7799, Timothy Stacey, SANS, September 22, 2000. www.sans.org/infosecFAQ/policy/standardization.htm

14. Survey Results, GAMMA, Gamma Secure Systems, Diamond House, Frimley Road Camberley, Surrey, GU15 2PS, UK www.gammassl.co.uk/bs7799/survey.html

15. Is it for you?, Gamma, Gamma Secure Systems, Diamond House, Frimley Road, Camberley, Surrey, GU15 2PS, UK www.gammassl.co.uk/bs7799/apply.html

Chapter 6

Conclusion

The Internet and office computer networks provide the ability to conduct research and exchange data much more efficiently that ever before. The advent of e-commerce brings a worldwide customer base to companies that could never afford to market their goods and services on a world wide basis. While these tools have revolutionized how businesses conduct their affairs, there is also the need to build computer security into how we connect to the Internet and structure our internal office computer networks. As mentioned previously, the hacker may find a more lucrative target in the small and medium sized business than attempting to attack the large company with well established computer security mechanisms. As a manager, you need to be aware of the threat to your Internet access and to your office computer network. Building computer security into an office computer network requires some time and resources. If you have an internal automation staff or rely on outsourced talent, you must provide adequate time for security. Too often manager's are told "We didn't close all the doors because we're too busy doing "real" stuff" and "If the hackers got caught, we didn't punish them. It would be too embarrassing to admit we got hit. Our Incident Response Plans were inadequate". [16] Providing the appropriate guidance, time and resources for computer security will prevent the successful attack or provide early warning that one is underway. Remember, ""Most of the successful system and network attacks exploit a small set of vulnerabilities." [17] Careful attention by your automation staff and management understanding and involvement towards developing computer security will allow you to maximize the benefits that the Internet and office computer network can bring to your business. Improving the security of your computers, computer network and Internet connections pays dividends for all businesses as "Our individual security depends on our mutual security."[18] A heightened awareness of the threat and how to defeat or minimize the damage that can be done will reduce the severity of future attacks.

This paper has attempted to provide a broad based look at the problem of computer security from the perspective of the small and medium sized business executive. There are entire sections of your local book store dedicated to the various topics we have covered. Should you desire more information, it is readily available in much more detail. This paper gives you the basics necessary to deal with your automation staff or contractors. Management understanding and involvement in computer security is required for effective implementation of any security program.

End Notes:

16. SANS Institute, Marchany, Randy and Craddock, Mary, "The Top 10 Internet Security Vulnerabilities – A Primer"

http://www.sans.org/audio/sanstop10presentation.pdf

17. Ibid

18. Ibid

References

- About.com, “The Downside of Network Security”, Jim Williams

- Gamma, “International Standards Organization Standard 17799, Survey Results”, 4/9/01

- Gamma, “International Standards Organization Standard 17799, Is it for you?, 3/6/01

- MacMillan Publishers, “Intrusion Detection”, Rebecca Gurley Bace, 3/12/2000

- Montreal Business Magazine, “Network Security: What are you waiting for?”, Daniel Tatone, 5/7/2001

- National Infrastructure Protection Center Highlights, “Healthcare: Access to Medical Information Files Requires Enhanced Security”, 3/23/01

- National Infrastructure Protection Center Highlights, “Computer virus protection: Layers of protection are key to safeguarding systems.” , 4/18/01

- National Infrastructure Protection Center Highlights, “Teleworkers: Increasing Risks to Corporate Infrastructures”, 4/18/01

- SANS, “The Top 10 Internet Security Vulnerabilities – A Primer”, Randy Marchany and Mary Chaddock

- SANS, “Toward Standardization of Information Security: BS 7799”, Timothy Stacey, 9/22/00

- Security Auditor, “What is ISO17799”, undated.

- Securing Wireless Networks, Joe Klemencic, 5/1/2001

- Xinetica, Ltd., “Corporate Information Security Strategy – how to avoid giving free information to attackers” Richard Bartley, 5/26/2001

Last Updated: July 27th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event