



The Software Group Limited

642 Welham Road
Barrie, Canada, L4N 9A1
Phone: (705) 725-9999
Fax: (705) 725 -9666
www.sentinet.net

Beyond the Fear, Uncertainty and Doubt

What you need to know about Internet Security!

Table of Contents

INTRODUCTION	3
WHO IS THE SOFTWARE GROUP LIMITED.....	3
WHAT IS THE INTERNET?.....	3
THE TERMINOLOGY	4
<i>Some Other Useful Acronyms.....</i>	5
THE THREAT.....	5
LOCAL VERSUS REMOTE EXPLOITS	5
WHAT HAPPENS WHEN A SERVER IS COMPROMISED?	6
THE GOOD NEWS IS "IT'S NOT THAT BAD"	6
THE SOLUTIONS	7
KNOWLEDGE AND PROCEDURE	7
REQUIRED COMPONENTS	8
<i>Firewalls with Packet Filters</i>	8
<i>The DMZ Network.....</i>	8
<i>VPN – Why and When</i>	9
<i>Hardened Servers.....</i>	9
<i>Intrusion Detection Systems</i>	9
THE NUMBER ONE KEY	9
<i>Vigilance.....</i>	9
<i>Who is watching it all and keeping it secure?</i>	10
CONCLUSION.....	10

Copyright © 2003, The Software Group Limited.

Trademarks:

All rights reserved for the respective owners of the trademarks listed below.

SentiNet™ is a Trademark of The Software Group Limited.

Introduction

Who is The Software Group Limited

The Software Group Limited is a leading supplier of high performance wide area networking solutions to the Internet, landline and wireless industries. Our products and services meet the needs of traditional and emerging telecommunications markets.

The Software Group Limited is a privately held Canadian corporation founded in 1982. The company's success can be attributed to excellence in technology, superior quality assurance and uncompromising customer support.

Our mission, then and now, is to provide products and services that optimize the functionality of legacy and next generation wide area networks for corporations worldwide.

For over than two decades The Software Group has been implementing Wide Area Network (WAN) protocols. Using our own technology we have maintained a static Internet connection since 1988 (pre-web), with custom-developed firewall software and Frame Relay.

The Software Group develops network protocols, at the code level, that are integrated with the operating system. All the engineers at The Software Group understand network protocols, especially TCP/IP, at the protocol level. This is a company of experts, whose mastery has been acquired through years of worldwide network implementation.

Small and medium sized enterprises will benefit from this expertise as much as global corporations. The Software Group is now looking to local needs. Even third-party off-the-shelf products require professional knowledge to install, optimize and maintain. The Software Group provides solutions, designers and people who understand the whole network, from the workstation through the server and on to the customer.

What is the Internet?

The Internet began as a virtual public network consisting of a collection of privately owned computers and networks from around the world that permitted the transportation of data across their interfaces from one location to another.

Eventually the volume of data transferred and equipment used for transferring data became so significant that companies could no longer afford to donate these resources and the commercial Internet was born. This remains a loose affiliation of several large Internet backbone providers and thousands of smaller Internet Server Providers (ISPs). There is no central authority, and most of the regulations and standard in the Internet are maintained and adjudicated through volunteer bodies and self-government by the backbone providers and ISPs.

The Software Group has recognized the Internet as an important tool, from its beginnings as a loose collection of asynchronous serial lines to today's ubiquitous web, The Software Group has always had a presence on The Net.

Moreover, The Software Group, itself a small enterprise, has always recognized a need for cost effective internetworking. At the beginning of the Internet era when the cost of routing over Ethernet and synchronous communications was exorbitantly expensive, The Software Group

developed a software-plus-hardware subsystem solution for workstations and servers (NetcomRouter). When The Software Group purchased its first dedicated Internet connection, the need for security was seen. Rather than purchase an expensive hardware solution we developed and implemented our own packet filtering firewall within NetcomRouter.

Our foresight paid off immediately when the firewall logs revealed hacker attempts within a week of implementation. Today those attempts occur within hours of a new Internet presence, and according to the logs The Software Group's Internet servers are probed thousands of times per day.

The Terminology

The Internet and networking technology both come with an abundance of buzzwords and acronyms. This table will define some basic terms found in this document.

- | | | |
|-------------------------------------|---|---|
| Packets | - | Information like files and databases are split into small pieces called packets to be transmitted over the Internet using TCP/IP protocols. Packets are used so that errors in transmission can be corrected quickly by re-transmitting the packet instead of the entire file. |
| Firewall | - | <p>A firewall protects your system from malicious intrusion. Packets of information arrive at your server. Without a firewall, the server will deliver the packet (which will become part of some files, databases, etc.) to the specified address. Once at its destination, the file is read. If the packet has been delivered to a system address and contains malicious code, the server and the network could be compromised.</p> <p>A firewall will not allow delivery of packets unless these packets arrive from a known address, through an acceptable channel to a specific destination.</p> |
| Router and Gateways | - | A router tells packets where they can travel through the network. The gateway is the router that serves the default route to the rest of the world. |
| DNS | - | The Domain Name Server (DNS) equates host and domain names to IP addresses. When the DNS is polled it will return an IP address for the name passed in. The domain name system is directly analogous to a phone book in the telephone network. However, as the network communication is often between computers rather than between people, the "phone book lookup" has been automated to speed computer to computer communication. |
| Vulnerabilities and Exploits | - | <p>Vulnerabilities are weaknesses or bugs in software.</p> <p>Exploits take advantage of vulnerabilities to do something, like crash the software or allow hackers to gain control of the machine the software is running on. For example some Internet worms and viruses take advantage of e-mail vulnerabilities to execute themselves. Once executed they may do nothing more than confirm your valid e-mail address to sell this information to marketing departments for Spam mailings or they may be much more invasive.</p> |
| Viruses, | - | A virus is program or piece of code that runs without the knowledge of the |

Worms and Spam

user and usually will perform malicious actions such as deleting files or using up computer resources. Viruses attach themselves to existing files (executables, MS-word documents, or other advanced file formats that are in themselves already executable in some way). Viruses are able to replicate themselves and infect other files.

A worm is a program that can run on its own. It can replicate itself over computer networks. Most worms begin by exploiting a vulnerability in an existing program on the machine, perhaps even as a virus. The difference between a worm and a virus is subtle and more a question of semantics.

Spam, on the other hand, is unwanted e-mail. Spam is usually nothing more than an irritant, but can also carry exploits, such as e-mail worms and viruses.

IDS

An Intrusion detection system monitors activity at some point in your network or computer. Trends in unusual packet activity, for instance packets arriving at unauthorized portals, may constitute an intrusion attempt and will be alerted as such.

Some Other Useful Acronyms

- CERT** - The **C**omputer **E**mergency **R**esponse **T**eam coordination center for worldwide response to security alerts and vulnerabilities
- ISP** - Internet Service Provider
- DMZ** - The DeMilitarized Zone is a buffer network implemented between a companies private network and the Internet. The DMZ is commonly used to host Internet services (e.g. a web site or transmission of e-mail). It is partially protected by a firewall, but partially exposed because of the services available to the Internet. Communication between the private network and the DMZ is strictly controlled and monitored.
- VPN** - Virtual Private Network is a type of network that runs over the Internet completely secured using encryption technology.
- TCP/IP** - TCP/IP incorporates two fundamental protocols used for Internet communication, Transmission Control Protocol and the Internet Protocol.

The Threat

Local versus Remote Exploits

The local exploit comes from machines that are part of your network, behind your firewall. Any user that has been granted some permission on your network may have enough ability to gain root access to your system, to exploit known vulnerabilities (for example in IMAP or CGI scripts) or simply physically attack servers (by turning them off or installing software at the console).

The remote exploit comes from the random hacker, who gains access to your network from the Internet through a known IP address and vulnerability. Other remote exploits might come from poorly written local scripts that a hacker could take advantage of remotely.

The first question that must be answered is whether you trust the users on your network. For large corporations, like banks and insurance companies, whose networks may have tens of thousands of users, the answer to this question would be NO. But, for small and medium sized businesses, the answer is probably YES.

Local exploits for these businesses come mostly in the form of physical intrusion. To ensure safety from these kind of threats, servers should be kept in a secured location and users must be taught secure shutdown procedures and proper password use.

Remote exploits must be dealt with differently. You must ensure your network is safe from random hacker attempts 24 hours a day, 7 days a week, 365 days a year.

What Happens when a Server is Compromised?

You may wonder why anyone would bother to attack a small company's server. The reason is that the attacks are automated, not targeted. Hackers search the web for known vulnerabilities to exploit. Through these vulnerabilities a hacker gains access.

There are several things that can happen to your network and your business when your server is compromised.

Some worms cause "Denial of Service" attacks, bombarding your IP address with thousands of packets, consuming bandwidth, making it impossible for other users to access your network, causing service interruptions or worse, crashing your server or ISP service.

Some attacks may give hackers coding access to your web site, allowing them to deface your Internet presence or giving them a launching pad from which to initiate attacks on other networks.

The most feared attack is that which gives a hacker access to your databases, compromising sensitive data.

All these types of attacks have a negative affect on your business and your business's image.

- **Loss of credibility.** Customers receiving viruses or attacks from your server perceive your business as a threat.
- **Loss of time.** The time required to reinstall software, rebuild servers and clean in-house networks can be considerable.
- **Loss of revenue.** If your Internet e-business is down you lose potential sales and customers.

The Good News is "It's not that bad".

The concept of a masterful super hacker outwitting the computer and overcoming the firewalls and encryption makes for a great novel or movie, but it's not how systems are attacked. The reality is much more mundane.

Vulnerabilities are simply flaws, or bugs, in the protection software. Sometimes these are simple oversights, just like a doorframe that leaves the locking latch bolt accessible making it easily

popped with a credit card or coat hanger. More often these vulnerabilities are much more complicated. Nonetheless, once the “trick” is known, it’s relatively easy to break in.

But it’s still a static system. Hackers have tools that identify software, look up known vulnerabilities, and test to see if the vulnerabilities have been left unfixed.

Organizations such as CERT make vulnerabilities known to developers immediately and to third-party system administrators simultaneously with updates and fixes.

In the five years of participation with CERT, The Software Group has not seen an exploit precede a vulnerability. This means that CERT has been able to identify vulnerabilities before a hacker could write malicious code to take advantage of it.

The biggest newsmakers of the last few years, the Internet Worm, Code Red, Nimda, and recently Sapphire, exploited vulnerabilities that had been **known and fixed** for months. The infected machines were neglected machines that had not been kept up to date.

The Solutions

The primary worry for small to medium businesses is random attacks from the Internet. As these are focused on static known vulnerabilities, it is relatively easy to defend against them with a few simple tools and processes.

Should you be worried about a focused attack, perhaps targeting your specific business and business information? Perhaps. Certainly if you collect credit cards numbers on the Internet, or if your systems store any information of immediate monetary value, you should. If you feel your business presents such a target, then you need more extensive security protection. A full security audit is the best place to start, because most protected systems are compromised from the inside rather than by unknown external attackers.

Knowledge and Procedure

Know your network and Internet requirements. The simplest connection uses the Internet only but does not provide services to the Internet. If you plan only to pick up your e-mail from the ISP, host your web site offsite and have others maintain your domain name, you can then protect your business with an easy-to-install, basic firewall.

However, this is an inflexible solution, and leaves you with little control. You may have need for more services than an offsite web site can handle (dynamic pages served by your servers perhaps). You may have telecommuters or travelling sales people that need access from outside.

Whatever services you wish to take under your control, you should document and define clearly. These are the services that need to be monitored and protected from the Internet.

Once you have defined what you want, define the procedure for maintaining it. Knowing which services are exposed, and how they are exposed, will allow you to monitor the news and vendors bulletins. Clearly define how users will access your network and the Internet and ensure the procedures are followed. Some essential procedures are as follows:

- All vendor installed passwords must be changed. All users and machines, especially exposed to the Internet, must have non-trivial passwords, consisting of a combination of

upper and lower case letters, numbers and special characters. These should be changed regularly.

- All user workstations should have a virus checker installed. Ensure virus signatures are updated regularly, preferably automatically. If you have an in-house mail server, consider a server based virus checker as well.
- Control or eliminate modem access to your office. Both incoming and outgoing modem should be curtailed. The fewer points of entry to your network, the easier it is to protect.
- Install security updates from your vendors immediately.

Required Components

There are several components your network will require to ensure security.

Firewalls with Packet Filters

The firewall is your front line defense against intrusion. Incoming packets must meet certain criteria before they are allowed into your network. The firewall packet filter verifies packets at several levels. With each assessment the packet can be allowed to pass onto the next check, forwarded to another address or dropped. The packet filter checks the interface the packet came in on, the protocol it is using, the source and the destination of the packet, and even the target service (port number) on the target machine

Computer systems today run dozens, even hundreds of *services* that make your office more productive. Many of these services are enabled by default, while many are enabled by installation of software without your immediate knowledge. A firewall operates by denying all those services, except the ones you specifically enable, to the Internet.

A firewall typically has two (Internet and Private Network) interfaces. Optionally there may be a DMZ interface. Larger firewalls will handle many network interfaces.

For example: If the packet comes to an interface that does not allow packet traffic, it is denied and the packet is dropped. If the interface does allow traffic, but not for the protocol specified, it is denied and the packet is dropped. If it is from a source that is not allowed or going to an unrecognized destination, it is denied and the packet is dropped. A specific example is a web server. Your organization may have decided to have their web site hosted offsite (quite common) but might still have in-house web servers running for private use. A firewall will intercept and block all Internet traffic destined for the in-house web server at TCP port 80.

The DMZ Network

The DMZ network is located between two firewalls and is partially accessible by the Internet and your internal network, but is separated from your internal networks by the internal firewall filters. The DMZ gives you a network that is accessible worldwide containing non-sensitive information, like forums, web sites and news. The two firewalls do not need to be physically separate devices; a single firewall appliance with multiple network interfaces can provide both the DMZ and external firewall functions.

VPN – Why and When

A VPN uses encryption to create a virtual private network tunnel running over the public Internet. This tunnel can be from one private network to another or from one user's machine to a private network. Users allowed access to the tunnel (e.g. employees working from home or Sales getting customer data from another country) can also access any or all of your sensitive data, allowing your network boundaries to reach around the world.

A VPN is not essential unless you need access to your internal network from home or another office.

For home users, Windows operating systems are delivered with single workstation VPN (PPTP) which is easy to configure and use. At your office, you will need a PPTP server to establish the tunnel.

For office-to-office VPN you are best served by a VPN device implementing IPSEC (IP Secure) protocol.

Hardened Servers

Servers are manufactured and shipped for ease of use and productivity. However, if a server is exposed to the Internet, the administrator needs to review all the applications and services enabled. The administrator must disable the unessential services and then verify that all known security holes are repaired or blocked in essential services. The administrator must ensure that the configuration of the provided services doesn't allow the machine to be compromised or used for purposes other than intended. This process is known as *hardening*. Hackers will not compromise a hardened server, which is properly monitored and maintained.

Intrusion Detection Systems

Some exploits, like those written into Active X scripts on web sites, can overwrite files on your system, replacing them with files that, if run, can be used by hackers or other malicious code. Some intrusion detection systems monitor your network server system files for changes and notify your administrator when files have been unexpectedly changed so that your network is not compromised. Other intrusion detection systems monitor a network's traffic looking for *signatures* (just as virus scanners do) that match known intrusion attempts.

Intrusion detection systems are typically used forensically ... after the attack has occurred. This information is still important, and can allow you to isolate infected machines quickly. Intrusion detection systems are evolving and newer systems are more proactive, taking action on intrusion attempts as they occur.

The Number One Key

Vigilance

Effective security is procedural, not just hardware and software related. Even with the best components money can buy, if no one is watching and updating then your network is still vulnerable.

Who is watching it all and keeping it secure?

To install a network server, DMZ server, firewall, VPN box and intrusion detection software from the ground up requires a trained technician. To configure, maintain and monitor this new network will require a network administrator. On top of this you will require anti-virus software to be installed on every user's computer and an ISP to configure a mail account for each user in your corporation and to host your web site.

However, it is no longer necessary to build and integrate all these components. A properly designed firewall will come with enough built-in rules to protect your internal network. Knowing what services you need and enabling/disabling others can be as easy as a mouse click on a configuration screen.

SentiNet Internet Management Servers are The Software Group's product line of servers that have some or all of these components in one easily managed box.



Install this box in your network and configure the required components from a standard web browser. You now have control. The robust default firewall will deny all packets unless a filter is explicitly created to allow it (for instance, incoming e-mail). Configure e-mail accounts for as many users as you need. Give some users Internet access and others only internal networking abilities. Purchase a domain name and post the web site yourself that same day. Have all your incoming and outgoing e-mail filtered by SentiNet so you don't have to maintain anti-virus software on all your computers. Now you can monitor all your components from one eternally vigilant machine: SentiNet logs and reports on Internet usage, mail and firewall activity, VPN and ISP connections, system file and network intrusion attempts.

While you are minding your network, The Software Group is minding your vulnerabilities. The Software Group monitors the hundreds of CERT notifications each month, knows which are applicable to SentiNet, and responds. Before you hear about an exploit in the media that will take advantage of a vulnerability, you will have received an update, often before the end of the same day that CERT posted the report.

Conclusion

The Internet offers low-cost, high-value networking unlike ever before. It's not a fad... it's a tool. It is an important and valuable tool that needs to be part of your business, just as a phone, fax, printer, computer and advertising are part of your business. The Internet is not a magic grail that will suddenly make you profitable and rich, nor is it a cutting edge technology for "early adopters". It's a proven, reliable and rich medium that needs to be carefully analyzed and conservatively adopted by responsible business.

Once connected to the Internet you will find a wealth of resources – marketing, technical and comparison-shopping – as well as many forms of communication (e-mail, teleconferencing, e-seminars, instant messaging, etc.). You will literally have access to the world, as every city in every country on every continent is available by Internet.

Peace of mind is not a matter of buying an expensive solution once. Peace of mind comes from having a sound management process in place to track your exposure to the Internet, to be aware of vulnerabilities, to know when they affect your network and where to get the necessary updates immediately. Only with this kind of eternal vigilance can you go beyond the fear, uncertainty and doubt of doing business on the Internet.