Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

GIAC Security Essentials Certification

Practical Assignment Version 1.4 - Option 1

Are You a Responsible Internet Neighbour?

Written by: Phillip Croft
15 August 2002

© SANS Institute 2000 - 2002 Author retains full rights.

1 Summary

Did you know that if you connect to the Internet you have a responsibility to protect others? You may not find it written in the manual that comes with your PC, server, router, firewall or SMTP mail software. Actually, if you have had little to do with PC's you probably haven't got any idea that someone is out there just waiting to use your systems and networks to reek havoc on your unsuspecting Internet neighbour. When people talk about security, they are usually talking about protecting themselves. They don't usually think about protecting their neighbour. However, when you join the Internet community, you have a responsibility to be a good Internet citizen.

You need to play your part in stopping the spread of Viruses, Worms and Trojans. Don't allow that email Spammer to use your SMTP mail server. If you're an ISP, don't allow your dial-up or permanently connected clients to send out false or malicious TCP/IP traffic. Patch that operating system or software. You shouldn't let others use you equipment to attack your Internet neighbour. Configure your FTP server so that it cannot be used for distribution of illegally copied software and files. Don't expose confidential information. Make sure you have a security policy.

2 Are You Irresponsible?

Do you allow others to use your SMTP Mail Server to relay Unsolicited Email?
Do you allow others to use your servers and workstations to perform Distributed Denial of Service attacks on your Internet neighbours?
Are you an Internet Service Provider that allows its customers to Spoof other addresses?
Do you allow people to store ill egally copied software and files on your servers for distribution to others?
Do you allow email viruses to leave your workstation(s), server(s) or company?
Are you allowing your staff to cause trouble for your Internet neighbours?
Are you a home user, or a n organisation, that hasn't invested any time in understanding how being connected to the Internet comes with responsibilities?
Do you have information, such as credit card details or other personal information, on your systems that have inadequate securit y protection?
Have you no basis for your security practices and solutions?

3 Your Responsibility

In this section I'll describe some actions and precautions that you should do to be a responsible Internet neighbour. This is not a definitive list, but it will cover the most common areas and it will certainly get you started on your way to doing you part to make the Internet more valuable for everyone.

Throughout this section I will refer to various products and resources. Use them as references and starting pl aces, but please do not presume that I specifically recommending them or have any affiliation with them. They are simply examples to help you start looking for solutions to meet your needs.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.1 SMTP Relay Spam

3.1.1 What Is It?

Firstly, let's make sure you know what Spam is. Unsolicited Bulk or Commercial Email is often referred to as spam. It refers to all those emails you get from people or companies you never communicated with, but somehow they managed to get your email address and start sending you email along with numerous others. You all get the same junk email you didn't ask for and probably don't want.

SMTP Relay Spam is fairly simple to understand. Email travels from the sender to the receiver by going through Simple Mail Transfer Protocol (SMTP) relay servers. If the SMTP relay doesn't do any checking of the validity of the sender, then the relay is considered an "Open Relay". Open relays simply forward whatever they receive. If you know of an open relay then it is very simple to send it as many emails destined for your unsuspecting recipients, as you like such that the sender information is invalid.

If you own or run an SMTP relay and it is an "Open Relay" then you are allowing anyone to use your server for SMTP Relay Spam.

If you want to find out more about relay spam have a look at this reference;
http://mail-abuse.org/rbl/rationale.html#RelaySpam

3.1.2 What Do You Do to Stop It?

There are a few things you can do to stop Spam going through your SMTP relay.

1. Configure your SMTP relay so that it isn't an "Open Relay"
2. Block email from other "Open Relay" servers
3. Use SMTP software that specifically has Anti-Spam features

The first option is quite simple and doesn't have any great negative impact on you. There are plenty of SMTP relay server software products (in fact most) that provide this by default or can be configured or patched to provide it. It's simply a matter of verifying that the source of the email is valid and if it isn't, block it.

The second option is to configure your mail server to use DNS-based blocking lists (DNSBL) and refer to one of the published lists of IP addresses known to forward Spam. You need to select your list carefully as the relay server doesn't distinguish between spam and genuine email coming from a black listed relay. You will need to shop around the various sources to select a list that meets your needs.

The third option incorporates the first two options and extends them. There are a number of software products that are appearing with the ability not only to use DNSBL filtering and the basic valid source check, but also to do very clever checking against email to determine if it is Spam or throttle the number of emails from a source to reduce the practicality of using the relay for Spam.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Some sources to have a look at are (This is by no means a complete list):

http://www.spews.org - The FAQ has one entry that list a number of list sources and they offer their own services. They also have many links to other sites and services. A very good place to start.
http://www.spamfaq.net/ - A good reference source with links to useful sites
http://ordb.org/ - Open Relay Database Service
http://relays.visi.com/ - Relay Stop List provided by visi.com
http://mail-abuse.org - Offer services to help you with Anti -spam
http://spamassassin.taint.org/ - Offer SpamAssassin, a mail filter to identify Spam.
http://www.spambouncer.org/ - Offer SpamBouncer, a mail filter to identify Spam.

3.1.3 How Does Stopping It Help You?

There are a number of reasons for stopping SMTP Relay Spam. Some of them are obvious and some are not.

Probably the most obvious reason for stopping SMTP Relay Spam, is to stop you being a target for Spam. If you don't let it in, you won't get it in you Inboxes.

If you don't configure your SMTP relay so that it isn't an "Open Relay", then you might find it on one of the DNSBL lists. This will impact your outbound email such that some mail may not reach its destination. A recent article called "Are spam 'blocklists' going too far?" talks about how big a problem Spam is and the issues of blocklists.

"Almost every company now is looking at using blocklists because there's no choice -- there's too much spam coming in," said Steve Linford, who maintains a London-based blacklist of mass e-mailers called the Spamhaus Block List. "The blocklists need to be run with an amount of responsibility and ensure that if any innocent user is caught on a blocklist there's a means to get off quickly." (Olsen)

Even if you never receive Spam, it is costing you money allowing others to use your servers for relaying and storing Spam.

- There's the additional cost of the bandwidth used on your Internet link.
- The cost of having a higher performance server than necessary or more than necessary disk capacity.
- The cost of your important outbound emails being lost because they were blocked.

You might also feel good that you are doing your bit to stop Unsolicited Bulk Email being sent to others, especially your business partners, via your email system. This could also be potentially very embarrassing.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.2 Egress and Ingress Filtering

3.2.1 What Is It?

Egress filtering is filtering of outbound TCP/IP traffic against various rules to ensure that the traffic that leaves your network is valid. One example is to verify that the source IP address is valid for the network it came from. What this does is stop computers on your network being used to attack other computers on the Internet using IP Spoofing. Other examples are to block traffic that can be "finger printed" as malicious, or gives away valuable information, etc.

Ingress filtering is filtering of inbound TCP/IP traffic against various rules to ensure that the traffic that enters your network is valid. It is very similar to egress filtering : only it is set-up on the inbound link of a network. Usually this will be set up on the ISP input link from a customer. As a good Internet neighbour the ISP would configure ingress filters so that its customers don't deliberately or accidentally become a source of a DoS attack by stopping source IP spoofing.

IP Spoofing is when an IP packet is sent using a different source address than the one the packet actually comes from. IP Spoofing is used to hide the real source of IP packets to enable anonymity of an attacker.

In a CNN.com article, Brian Livingston writes;

"Every ISP can prevent incoming packets with false IP addresses from being passed on (this is called ingress filtering). And every corporation with an Internet connection can ensure that spoofed packets don't leave the corporate network. (This is called egress filtering." (Livingston)
URL: http://www.cnn.com/2000/TECH/computing/03/01/prevent.ddos.idg/index.ht ml

Typically, egress filtering is used to prevent system on your network participating in Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks against systems on the Internet. Ingress filtering is used to prevent ISP's customer systems on the customer's network participating in DoS or DDoS attacks against systems on the Internet. Attacks such as SYN Flooding and SMURF attacks being common examples. Two other specific examples are recorded in the "Perle Security Advisory - Vulnerabilities of Simple Network Management Protocol (SNMP) Messages" and "CERT® Advisory CA -2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)" . These advisories describe how SNMP vulnerabilities can be exploited to produce a DoS attack and how egress and ingress filtering can be used to prevent it.

3.2.2 How Do You Do It?

Egress filtering is simply a matter of configuring your outbound router or firewall with access lists that define what is and isn't allowed to leave y our network. Ingress filtering is simply a matter of configuring your inbound router or firewall with access lists that define what is and isn't allowed to enter your network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

There are some very basic rules that should be applied in egress and ingress filters:

- Never allow traffic out to the Internet with a source address from one of the Private Address Space blocks defined in RFC 1918.

  "Address Allocation for Private Internets – RFC 1918

  3. Private Address Space

  The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0	-	10.255.255.255	(10/8 prefix)
172.16.0.0	-	172.31.255.255	(172.16/12 prefix)
192.168.0.0	-	192.168.255.255	(192.168/16 prefix)" (Rekhter, P.4)

  Here's a more extensive list that comes from "Help Defeat Denial of Service Attacks: Step-by-Step".

"0.0.0.0/8	- Historical Broadcast
10.0.0.0/8	- RFC 1918 Private Network
127.0.0.0/8	- Loopback
169.254.0.0/16	- Link Local Networks
172.16.0.0/12	- RFC 1918 Private Network
192.0.2.0/24	- TEST-NET
192.168.0.0/16	- RFC 1918 Private Network
224.0.0.0/4	- Class D Multicast
240.0.0.0/5	- Class E Reserved
248.0.0.0/5	- Unallocated
255.255.255.255/32	- Broadcast" (Krause)

- Never allow traffic out to the Internet with a source address that is not from one of your internal network address blocks or from the customer's allocated address blocks.
- Never allow SNMP traffic out to or in from the Internet
- Configure your perimeter router for "disable forwarding network-prefix-directed broadcasts" as a specific measure against participating in attacks such as "Smurf"
- Log any packets that do not match the rules to allow it out. You will need this to set up notification when it occurs, so that you can immediately start tracking down the source.

There will be exceptions to the rules above, where it is valid to allow specific traffic out to the Internet. Typical examples are when you are an Internet Service Provider (ISP) that is routing traffic through your network. However, even an ISP that has dial-up customers should not allow this traffic to leave their dial-up network segment, as this prevents their customers misusing the ISP's network.

There are other more specific filters that could be configured. You will need to research security sites and know a lot more detail about your own network to determine what specific filters to configure. Look for vulnerabilities in systems that can potentially be used for DoS or DDoS attacks.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Every router and firewall is different in the way you configure the filters and access lists. Rather than reproduce every possible configuration, I simply direct you to the vendor's web site and documentation to suit your specific device. Search for how to configure egress and ingress filtering. If you outsource you network perimeter device management, ask your service provider to do it for you.

For individuals, personal firewalls can provide egress filtering.

3.2.3 How Does It Help You?

The major benefits of implementing egress and ingress filtering are around restricting network traffic in and out of the networks for which you have responsibility. It certainly makes attackers easier to find and in deed alerts you to compromised systems being used as attack agents.

It also saves you the embarrassment of contributing to attacks on your Internet neighbours and partners, which can damage your corporate image and business relationships. Also, anytime yo ur resources are used in an unauthorised manner it costs you real dollars in used bandwidth and system resources as well as the cost of cleaning up a problem that could have been avoided or at least minimised. As you will see, these will become a theme in this paper.

DDoS is a particularly important problem as is highlighted by a recent CNN.com news article. The introduction writes;

"(IDG) -- Denial-of-service (DoS) attacks continue to present a significant security threat to corporations two years after a spate of incidents brought down several high - profile sites, including those of Yahoo! Inc. and eBay Inc., users and analysts report." (IDG)
URL: http://www.cnn.com/2002 /TECH/internet/04/09/dos.threat.idg/index.html

3.3 Security Vulnerabilities

3.3.1 What Are They?

According to Microsoft "A security vulnerability is a flaw in a product that makes it infeasible – even when using the product properly – to prevent an attacker from usurping privileges on the user's system, regulating its operation, compromising data on it, or assuming ungranted trust." (Culp, Scott). A bit wordy, but not a bad definition.

The problem with security vulnerabilities, from a "Responsible Internet Neighbo ur" point of view, is that many of them enable an attacker use your system(s) to attack someone else, as in the case of Distributed Denial of Service attacks. This gives them far more systems to perform the attack from. There are also attacks where the att acker uses someone else's system to do the attacking in order to maintain anonymity. Security vulnerabilities can also be used to steal confidential information. As an example, Daniel Sieberg from CNN.com responded to a question during an online chat session;

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

"CHAT PARTICIPANT: How high is the potential for stolen information from major online companies?

SIEBERG: With Code Red II, it really depends on whether they installed the patch and installed it correctly. Most major companies have likely taken the correct steps, but if a firm hasn't, a hacker could obtain information stored on that computer quite easily." (Sieberg)
URL: http://www.cnn.com/2001/COMMUNITY/08/07/sieberg.ot sc/index.html

3.3.2 What Do You Do to Fix Them?

First, you need to realise that they exist in just about every piece of software, from the operating system of a PC, to router software, to the applications running on the system. Once you realise this, you need t o take the issue seriously enough to do something pro-active about it. Being pro-active is the only way to truly be a responsible Internet neighbour. Just re-acting means you have let yourself become a problem to someone else already.

You need to put a process in place to identify, analyse and appropriately test and deploy fixes to security vulnerabilities as well as implement other solutions that mitigate the vulnerabilities where possible.

If you are an organisation, you need to have those firewalls in place. Have a security patch management process in place. Deploy intrusion detection tools at the perimeter of your network and on the most vulnerable hosts. Have a managed anti-virus solution in place. In the case when a system has been compromised, you n eed to go about identifying how it happened, what the compromise was, cleanup fully and stop it happening again. The "stop it happening again" is very important. If you have been compromised once, unless you change something it is certain to happen again. While your doing the forensic analysis, you should also try to determine whom else this could affect and make sure they are informed. If you don't do this, it is a bit like finding out that a type of lock is faulty and not telling the folks next door with the same type of lock.

If you are a single home PC user, this means you should run some kind of personal firewall and regularly check the web sites of the vendors of the software you use for security vulnerability notifications and their fixes. Then you n eed to keep your software patched regularly. You should also run good anti-virus software as they often detect malicious software that is aimed at exploiting known security vulnerabilities.

Let's get to some examples and be a bit more specific to help get you on your way. A typical scenario is the home user with a permanent connection to the Internet. These folk are prime targets for exploitation of security vulnerabilities in an effort to use their system to attack their Internet neighbour. These systems are permanently connected at good speeds and frequently unprotected against attacks. These people really need to have a personal firewall install and the most well known is probably

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Zone Alarm. Firstly, it will stop attacks from the Internet trying to exploit a security vulnerability on your PC and secondly, if you get compromised somehow (e.g. an email with malicious software attached) it will tell you that your system is trying to connect to the Internet in a way you wouldn't be expecting. One really good thing about Zone Alarm is that it's free. There are other personal firewalls available and it may be worth checking them out to see if one of them suits your situation better.

You need to patch Internet Explorer or whichever Web Browser you use and your operating system. For Microsoft products the best way to do this is to use Windows Update to regularly check for security and critical updates that apply to your system. For other products you will need to find the easiest way to keep your system up to date.

You need to have and keep you anti-virus software up to date. Buy the subscription so that your system can automatically download new anti-virus definitions.

As mentioned earlier there are a number of things organisations can do to help mitigate the risk of security vulnerabilities. Let's look however, at directly dealing with them. Security Patch Management is the key. It isn't enough to just try and block attacks getting to your vulnerable systems. This is just the start. Sooner or later the attackers are going to get past these defences and directly attack your systems. Your systems need to be patched to remove the vulnerabilities, so that even if some bad guy does get to the system they still can't claim it for their own and start using it for their own purposes.

Security Patch Management needs to be well executed. You need to have people whose job it is to monitor the numerous security notification services and assess the risk to your organisation of the notifications. Then you need people whose job it is to plan, test and deploy security patches to systems. You also need to have defined categorisations of vulnerabilities to set implementation timelines to match the risk assessment. To back all this up you need policies and auditing to define how your organisation deals with security vulnerabilities and verify that your organisation is indeed adhering to the policies.

3.3.3 How Does Fixing Them Help You?

Security Vulnerabilities can be used to attack your systems directly. This must not be forgotten. However, from a "Responsible Internet Neighbour" point of view, if you fix security vulnerabilities in your systems, then you not only stop others using your systems to attack your Internet Neighbour, but you also stop them using your systems to attack you even further.

Imagine you're a home user that pays per megabyte of bandwidth to the Internet used. Then imagine your PC has been compromised and it is now under the control, unbeknown to you, of someone who has set up an FTP server on your system and stores CD images and other files on you system. Then they tell people how to get the files from your system. Suddenly, your Internet connection becomes very expensive

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

and probably seems slow. Not only are you allowing someone else to trade illegal software and files, but also your costs and system performance are severely affected.

Now let's assume you're an organisation that operates a web site where customers purchase goods and services by credit card. You think you've done the right thing by putting the credit card details on a database server secured behind a firewall. You didn't however; manage the web server or the database server from a security vulnerability point of view. Now let's consider an attacker wanting to steal the credit card information. First th ey compromise the Web Server using well -known security vulnerabilities in MS Internet Information Server or any web server for that matter. With it they manage to get full control of the Web Server. It doesn't take too much for them to determine what datab ase software is in use. Then they use yet another well -known security vulnerability, this time in the database software, to send queries to retrieve information from the database server. Pretty soon they have got all that valuable credit card information o f your customers and you didn't do enough to stop them. What is that going to cost you in public image, lawsuits, and lost business? Your customers and business partners are your Internet neighbours and they are the people that keep your business in busine ss. You had better protect them properly or expect to go out of business.

3.4 Anti-Virus Protection

3.4.1 What Is It?

Most people have heard of computer viruses but may not be aware that viruses, worm and Trojans can play an important role in delivering malicious so ftware that can be used by an attacker to execute Distributed Denial of Service attacks on other computer systems.

Symantec Corporation, one of the worlds leading computer security companies, describes how anti -virus software plays its part in stopping DD oS attacks;

"**How can antivirus software help against DoS?**
Antivirus software detects viruses; it does not detect DoS attacks. However, it can play an important role in detecting the Zombie agents.

Antivirus software detects virus programs using a predef ined signature. Often, tools such as TFN or Trinoo execute their attacks from compromised computers that have Zombie agents on which they are secretly installed. Zombies are not just the victims of the DoS attack, but they are used to perform the actual at tack. By extracting a pattern or a signature from known Zombie agents, antivirus products can detect malevolent software on the compromised system. Antivirus software may also detect when a hacker is secretly installing Zombie agents. As of Feb 18, 2000, N orton AntiVirus can detect some common DoS agents such as TFN, TFN2K, Trinoo, and Stacheldraht."
(http://securityresponse.symantec.com/avcenter/venc/data/dos.attack.htm l)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Anti-virus software uses the same techniques to detect the malicious software that makes the Zombie agents as it does for normal viruses, worms and Trojans. Some examples of such malicious software, as categorized by Symantec's Virus Encyclopedia (http://securityresponse.symantec.com/avcenter/vinfodb.html/), are:

- IRC.Mimic
- W32.Storm.Worm
- W32.Dos.Trinoo
- W32.DoS.funtime
- Solaris.DoS.stacheld.c
- Solaris.DoS.stacheld.t
- Solaris.DoS.stacheld.m
- Smurf
- Hacktool.DoS

Something else you need to keep in mind when it comes to anti -virus protection and being a responsible Internet neighbour is that just because you are being attacked by a virus, worm or Trojan, doesn't mean that you should allow the attack back out of your systems and continue its propagation. You have a responsibility to stop viruses, worms and Trojans from not only entering your systems, but also from leaving them.

3.4.2 How Do You Do It?

There are many places in a network wher e anti-virus software needs to be deployed. The most commonly understood place is on user's computers. But this is not the only place that it should be deployed. Viruses, worms and Trojans can get into you systems in a number of ways, such as:

- Incoming and outgoing email
- Web Browsing
- Attacks on security vulnerabilities
- File sharing

In some of these cases, the virus, worm or Trojan never actually gets or needs a user's computer. As an example, the "Code Red" Worm attacked MS IIS Web servers directly.

So, you need to have anti -virus protection solutions at all point of entry to and exit from your networks. You should consider implementing mail server scanners, such as Sophos MailMonitor from (http://www.sophos.com). Implement Web scanning using a product such as WebSweeper from ClearSwift (http://www.mimesweeper.com). Another option is to get a combination product such as InterScan VirusWall from Trend Micro (http://www2.trendmicro.com/US/Products/Internet+Gateway/InterScan+VirusWall/default.htm) that combines email, web (http and ftp) and malicious mobile code (Java and ActiveX). Implement a managed server and workstation based anti -virus product such as Norton Anti -virus Corporate Edition from Symantec Corporation (http://www.symantec.com).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

If you're a home PC user or small business then you still need to protect all entry and exit points to your systems. However, this may best be accommodated by a combination product like "Norton Internet Security 2002 – Suite" from Symantec Corporation (http://www.symantec.com/sabu/nis/nis_pe/) or a selection of anti-virus products to suit your needs.

Whatever your size, from a single PC at home to a multi-national corporation, you need to implement a complete anti-virus solution that easily manages updates to stay protected and covers all virus, worm and Trojan attack vectors.

3.4.3 How Does It Help You?

Anti-virus protection implemented in your organisation means that you reduce the likelihood of being a victim of a virus, worm or Trojan, which not only means your system and data availability and integrity is not impacted, but you don't end up in the news as one of the organisations that had to shut down their computer systems to combat an attack.

As an individual you stop the propagation of these viruses and minimise the damage they can do to your computer and data. They can crash/trash your entire system and as a home user you are probably the least likely person to have backups of your data.

Also, the people and companies you deal with will be less than happy about receiving a virus, worm or Trojan from you. This impacts their perception of you or your organisation.

3.5 Web Site and FTP Security

3.5.1 What Is It?

Web and FTP servers often contain information provided to your organisation by others. As such you have a responsibility to protect that information from others that should not have access to it.

Allowing others to store files on your FTP servers without your knowledge means that you are leaving your servers open to use by others to store and distribute illegal software and files.

Web Site and FTP security is about securing access to information on your systems to protect both your data and the information others have entrusted to you. This means authentication, encryption and access control is necessary.

3.5.2 How Do You Do It?

If you are going to operate a Web Site that will contain confidential information, such as credit card details, or personal information, then you better make sure you deploy encryption and authentication mechanisms to protect it. You need to secure the communication with the server to stop others capturing the information being transferred between your server and the client and you need to make sure you select a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

technology that is publicly well accepted as secure for the purpose you are going to use it for.

The most common encryption for communication between a client and a server over the Internet is the Secure Sockets Layer (SSL) protocol. There are different levels of encryption with SSL and you need to select the strength to match the type of data it is to protect. There are other methods of encryption and you will need to investigate the options available to meet the security need you have.

There are many methods of authentication to control access to information, just as there are many methods of encrypting the data and again you need to select the technology that matches the security requirement based on the type of data being protected and the solution you are trying to provide.

You need to implement access controls to th e data and storage areas on your servers or you will find others accessing data and files they should not or storing data and files they should not. Don't forget to include auditing. You do need to know who is accessing data on your servers and when someon e is trying to break into your systems. You might need this information to assist in prosecution.

I am not going to try to explain all the methods of securing web and ftp servers, or any other server or Internet Service for that matter. What I do want you to take from this, is that there are many publicly accepted solutions to authentication, encryption and access control that you must investigate and evaluate against your data security requirements, and implement the most cost effective suitable solution to match the type of data you are protecting, especially if it isn't your data. Investigate Best Practices for securing Internet Services and if you are writing your own code, then these best practices need to include this. You don't want to be introducing your own vulnerabilities just because you didn't use "Best Practices" in writing your code.

This is probably the one security area that you need to consider employing a professional in the field to help you determine what meets your needs, such as security consultants, or qualified permanent security staff.

3.5.3 How Does It Help You?

Theft of private and confidential information from your systems is possibly the most costly issue you or your organisation can face, especially if it was someone else's information and not yours. The legal and corporate image costs could put you out of business. Loss of trust by your friends, business partners or customers is extremely hard to recover.

Unless you secure your web and ftp servers you leave yourself open to others us ing your Internet connection bandwidth and server capacity for their own purposes and you are paying the bills. You could also find yourself in legal problems and embarrassing media reports when it is found that you are allowing illegal activities to be carried out on your servers. Anything from storing "pirated" software, audio and video files, pornography, or any kind of stolen or illegal electronic data.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.6 Security Policy

3.6.1 What Is It?

According to RFC2196, "A security policy is a formal statement of the rul es by which people who are given access to an organization's technology and information assets must abide." (Fraser, P6)

A Security Policy is a document that your organisation uses to communicate its security goals to its users and staff, using as set of security guidelines. It is also the baseline to audit security practices with respect to computer systems and networks and is the basis from which all solutions to security concerns are derived to ensure that they comply with the policy.

A security policy is not only required with respect to being a responsible Internet neighbour, rather, it is more broadly required as the basis to protect company and technology assets. With respect to being a responsible Internet neighbour however, the security policy mus t include rules relating to security practices that if followed will not only protect your own company directly, but will also protect it indirectly. This means that the issues presented in this paper should come from the basis of the company security poli cy, where the goal is to mitigate the negative consequences of allowing people and systems to be part of poor Internet citizen behaviour.

3.6.2 How Do You Do It?

You're going to need a "Security Policy Development Team". To write an effective security policy req uires input from all stakeholders such as company management, technical staff, legal and security administration staff, etc. It is essential that the policy be written in consultation with these people to ensure that it will have corporate management suppo rt. Without this support the security policy will be useless.

Writing a security policy from scratch is a hard task and certainly more than anyone would want to do if they didn't have to. Thankfully, there are many places you can go to get started. I strongly recommend that this is the approach you take, as just about everything you will need to cover has already been covered by someone else. So, there should only be the need to invent components that are so specific to your organisation that you can't fin d an example and the rest should be more a matter of tailoring, combining and enhancing examples that are freely available.

Start from the basics by reading the RFC2196 - http://www.ietf.org/rfc/rfc2196. txt, have a look at "The SANS Security Policy Project" web site at http://www.sans.org/newlook/resources/policies/policies.htm and read "A Short Primer for Developing Security Po licies" at http://www.sans.org/newlook/resources/policies/Policy_Primer.pdf . Also, search around the Internet using "Security Policy" in your search criteria for samples.

You may want to consider employing a Security Consultant to assist in the development of the policy. This could speed up the process of developing the policy and may be especially helpful if skill level is low in this particular area in your

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

organisation. You may also need to consider giving staff, whose role it is to perform security administration and management, specific security training.

3.6.3 How Does It Help You?

Without a corporate management supported security policy there is no basis to work from to implement security solutions and practices. There is therefore nothing to measure your success against and no guiding principal for your users and staff to work from.

The security policy enables your organisation to effectively protect its technology and information assets. Its value is significantly broader than just the basis by which your organisation should conduct itself as an Internet citizen. In fact, this is undoubtedly the document(s) that underpins your entire organisation's security position and being a responsible Internet neighbour is but a small part of what the security policy enables.

4 Conclusion

You might think that a lot of what I have covered is about security management of your own organisation. However, although much of what I have written applies to protecting your own organisation or yourself for that matter, it is all particularly focused on being a "Responsible Internet Neighbour". It isn't enough to just be internally focused. Equally, it is not enough to just try to externally focused and assume that that will be enough to protect yourself as well. There are numerous other security risks that need to be addressed to protect you or your organisation. So, you need to start with your organisations "Security Policy" and incorporate security practices into it that support being a "Responsible Internet Neighbour". Then you need to actively implement these solutions and practices.

It is too easy to concentrate on security management purely from the point of view of protecting you or your organisation and forget about the greater role you have to play in security management and protect everyone on the Internet. After all, the true value of the Internet is the collective value it brings by connecting people and organisations together and unless you or your organisation do your bit to protect each other, you are undermining the true value of the Internet.

So you need to identify all those attack vectors from the various malicious activities on the Internet and implement policies, procedures and solutions that protect both you and the wider Internet community. That way you are being a Responsible Internet neighbour, not just someone looking out for them.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5 References

Angus, Fiona. "Spam gangs stalk the Net." Australian Personal Computer. August 2002: Pages 18-19.

Farmer, James. "The Evils of Spam", Last Modified: 04 -Jun-2002, URL: http://www.spamfaq.net/spam -evils.shtml (24 July 2002)

"Email Filtering", URL: http://www.spews.org/filter.html (24 July 2002)

Olsen, Stephenie. "Are spam 'blocklists' going too far?", 15 July 2002. URL: http://www.zdnet. com.au/newstech/communications/story/0,2000024993,20266 689-1,00.htm (14 August 2002)

"Open Relay Database FAQ", URL: http://ordb.org/faq/ (24 July 2002)

Guelfi, Michael. "Who's In Charge Around Here", URL: http://www.colmancomm.com/news/20020114_egress.htm (3 July 2002)

"Egress Filtering v 0.2", 2/29/00, URL: http://www.sans.org/y2k/egress.htm (3 July 2002)

Gibson, Steve. "Distributed Reflection Denial of Service", February 22nd, 2002. URL: http://grc.com/dos/drdos.htm (3 July 2002)

Krause, Mark. "Help Defeat Denial of Service Attacks: Step -by-Step", Last modified: 28-Apr-00 URL: http://www.mitre.org/research/cyber/DDOS/index.html (24 July 2002)

Livingston, Brian. "We can prevent those distributed denial of service attacks with 'egress filtering'", 1 March 2000. URL: http://www.cnn.com/2000/TECH/computing/03/01/prevent.ddos.idg/index.html (14 August 2002)

"CERT® Advisory CA -2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)", Original release date: February 12, 2002, Last revised: Tue Jun 25 12:32:57 EDT 2002, URL: http://www.cert.org/advisories/CA -2002-03.html (24 July 2002)

"Perle Security Advisory - Vulnerabilities of Simple Network Management Protocol (SNMP) Messages", URL: http://www.perle.com/support/snmp_advis_ory.html (3 July 2002)

Ferguson, Paul. and Senie, Daniel. "RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", May 2000, URL: http://www. ietf.org/rfc/rfc2827.txt (3 July 2002)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Culp, Scott. "The Definition of a Security Vulnerability", December 2000,
URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/vulnrbl.asp (24 July 2002)

Sieberg, Daniel. "Daniel Sieberg: 'Code Red' II worm attack", 7 August 2001.
URL: http://www.cnn.com/2001/COMMUNITY/08/07/sieberg.otsc/index.html
(14 August 2002)

"Denial of Service Attack (DoS)",
URL: http://securityresponse.symantec.com/avcenter/venc/data/dos.attack.html
(1 August 2002)

IDG. "Denial-of-service attacks on the rise?" 9 April 2002.
URL: (http://www.cnn.com/2002/TECH/internet/04/09/dos.threat.idg/index.html
(14 August 2002)

Carpenter, Jeff; Dougherty, Chad; Hernan, Shawn. "CERT® Advisory CA -2001-20 Continuing Threats to Home Users", Last revised: July 23, 2001.
URL: http://www.cert.org/advisories/CA-2001-20.html (9 August 2002)

"Symantec Product Web Page", URL: http://www.symantec.com/product/
(1 August 2002)

"Sophos MailMonitor Product Info".
URL: http://www.sophos.com/products/software/mailmonitor/ (1 August 2002)

"Google Web Directory of Anti-virus products",
URL: http://directory.google.com/Top/Computers/Security/Anti_Virus/Products/
(1 August 2002)

Farrow, Rik. "DDoS Is Neither Dead Nor Forgotten", 02/05/01.
URL: http://www.networkmagazine.com/article/NMG20010125S0003
(9 August 2002)

Huegen, Craig A. "THE LATEST IN DENIAL OF SERVICE ATTACKS: "SMURFING" DESCRIPTION AND INFORMATION TO MINIMIZE EFFECTS", Last Update: Tue Feb 8 17:47:36 PST 2000. URL: http://www.pentics.net/denial-of-service/white-papers/smurf.cgi (9 August 2002)

Fraser, Barbara (Editor). "Site Security Handbook", September 1997.
URL: http://www.ietf.org/rfc/rfc2196.txt (9 August 2002)

Rekhter, Yakov. "Address Allocation for Private Internets", February 1996.
URL: http://www.ietf.org/rfc/rfc1918.txt (9 August 2002)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

"The SANS Security Policy Pro ject",
URL: http://www.sans.org/newlook/resources/policies/policies.htm (9 August 2002)

Guel, Michele. "A Short Primer for Developing Security Policies", Copyright 2001.
URL: http://www.sans.org/newlook/resources/policies/Policy_Primer.pdf
(9 August 2002)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.