Global Information Assurance Certification Paper

Small and Mid size companies and Education

With the growing number of small and mid size companies connected to the Internet, so has the number of hackers and harmful viruses and Trojans. The problem is lack of education within these users. Hackers are coming more aware of the lack of security and personnel that smaller companies can afford to put into place.

As more and more companies are getting on the Internet, security is becoming more and more of an issue. The lack of training and understanding about security and protection is not put in place, until a problem occurs. It is much like viruses' 8 years ago, when nobody was running protection, because they did not think it was possible for them to be infected by a virus. Companies and home users were not concerned at all about the possibility of a virus attack. Now over the past 3 years having anti virus protection on your workstation and server have become just as important as running a word processor or spreadsheet program.

Smaller and mid size companies are not taking the proper precautions to make sure that they have adequate protection in place to protect against hostile outside attacks, and even inside attacks. Part-time or untrained personnel are running these environments, and not putting the proper equipment or software in place to protect the organization. The mind frame with many companies is that they only use the Internet for email. Over the next few years, these will be the companies that will get hit hard.

Hackers will grow tired of trying to get into large and major corporations that have the proper routers, firewalls, DMZ and other application in place in their perimeter that keeps these attacks from happening. Most corporation that do have the proper reporting and staff to watch for these attacks never know that it has happened to them.

A lot of the small and mid size companies often use ISP's as their provider for Internet access. These services do provide the company with access, but might not always provide them with adequate protection. The level of security that these organizations provide is typically unknown to the home user or small business.

One of the most important steps, is to make sure that you have properly trained people on staff that have some sort of certification in the security industry or has been to some classes. There are all types of different certification in the market. The most common ones are SANS and CISSP. Training not only helps in becoming aware of the various security problems in the industry, but it also helps in planning and creating policies to put in place. Training is only the start to the problem that companies face. There is an on going awareness that needs to occur with security. With the constant change of technology, so are the types of threats. Some companies are putting together web based basic security fundamentals for their staff to complete before doing certain jobs.

Another way of checking to see how secure your environment is can be done by security checkups. These checkups consist of anything from running vulnerability assessments to making sure that you are running the latest in virus definitions. There are tools available on the Internet or can be purchase from vendors that will allow you to assess your systems and networks just to see

how vulnerable they are. These tools run test just like a hacker would to penetrate your company. These tests include Denial of Service (DOS) attacks, which is a common one that hackers use to bring down organization networks and servers. Information scans that hackers use to gain information about your company before planning an attack.

Other holes these tools can check for are passwords that can be guessed or cracked. If shares exist that can be accessed, and if someone can FTP into your network without a password. Other vulnerability these programs can test for is Ping Floods, Send Mail bug's Trojan Horses and flaws in the operating system that can be address by patches.

If performing an assessment is not something that you fell comfortable doing there are organizations like (FoundStone) that can help you with these vulnerability assessments. Usually they starts out by doing some data gathering, and looking for reconnaissance information. Some of the kinds of data the auditor will look for are such things as trying to retrieve your routing table, trying to see if they can obtain ICMP netmasks,blooking for IRC servers, looking for SSH configuration information. Other kinds of things they will try will be checking for include an assortment of vulnerabilities associated with file transfer protocols, hardware peripherals, hacker Trojans and backdoors, SMTP and messaging problems, network file system vulnerabilities, website and CGI holes. and UDP ports. Security Vulnerability Assessment helps you manage customer expectations

Other measures corporations can take are by adding firewalls to their network. Firewalls come in different flavors. Application Firewall usually acts as a proxy server which relays or "proxies" connections from one system to another. These types of firewalls monitor applications (Raptor Firewall). Proxy/Circuit level Gateways proxies' connections from one system to another, but generally does no application checking (Gauntlet Firewall). Packet Filter Firewalls Host or router checks rules against an access control list (ACL). Generally, it filters on four different types of attributes. 1. Source address 2. Source port 3. Destination address 4. Destination port. The last type of Firewall is the Stateful Inspection type that is similar to packet filtering but performs additional checks. It keeps track of TCP sequence number, and matches outbound request to inbound traffic (CheckPoint, Cisco). "Small businesses should request quotes for managed firewall and intrusion detection services from ISPs. Those types of services usually cost less than the equivalent salary of a half-time firewall administrator"

If implementing an IDS or firewall is not in the budget, or the personal is not in place to maintain it, there are vendors that make personal firewall products that can protect and individual computer or server. Just like the big brother, these firewalls come in all different types as well. The most popular place for these type of firewalls or with business or home users that has cable modems or DSL. These personal firewalls are very straightforward and do not require a lot of security knowledge in setting them up or maintaining them. Personal firewall protection should not be considered an optional software accessory, in my view. Like antivirus software, it should be among the first additions to your computer operating system Carnegie Mellon's Software Engineering Institute, which tracks only a fraction of the world's computers, reports that there were more than 35,000 reports of computer security breaches last year affecting more than 4.3million computers.

One of the biggest threats that has hit businesses of all sizes, and has cost millions of dollars in down time is a virus. Businesses have suffered a lot of this year because of several email viruses. Most of these viruses can be stopped with the proper protection put in place. Having a scanner scanning your desktop or server is just the start. By the time, the virus hits the desktop; the email with the attachment is now in your mail server. To have been able to stop these viruses from entering the workplace, you need to stop them at the firewall or before the mail server. The best protection is to have a virus scanner scanning incoming SMTP traffic. You want to look for one that can not only repair viruses but also block attachments based on subject line or attachment name. Most of the Trojans and back door applications travel in email, if they can be stopped before they get into the workplace you have done half the battle of protection.

With all of the various different types of security products available, these products are only as good as the people who use them and understand them. With the growing number of automated tools on the Internet, so is the number of script kiddies and hackers. Having someone trained on staff that understands these issues is the biggest step a company can take to protect themselves, and the customers that depend on them. The key to good education of any kind is practice and repetition "People seem to feel that security is something you buy -- it's not a product, it's a process.

With the latest break-in at Microsoft , proves that know matter how secure you think your environment is, there could always be a hole. With proper training of employees and security awareness, these holes can be closed.

1. Internet Security Advice for Small and Midsize Enterprises
Relevance: 1.00 • March 08, 2000 • Source: Gartner Analytics • SPA-10-5787 • J. Browning; J. Pescatore]
http://gartner12.gartnerweb.com/en/sbin/ggrecord?NS-search- set=/search/set.11026.19.21&NS-doc-
2.Internet Security Advice for Small and Midsize HCOs
[Relevance: 1.00 • October 30, 2000 • Source: Gartner Analytics • SPA-12-3440 • J. Browning; W. Rishel]
http://gartner12.gartnerweb.com/en/sbin/ggrecord?NS-search-set=/search/set.11026.19.21&NS-doc-
3. Half of small & medium companies will suffer Internet attack
by David Legard, IDG News Service\Singapore Bureau http://www.security-informer.com
4. Security tests for employees scrutinized at conference
http://www.security-informer.com/ic_273442_3494_1-1474.html

Colin Gibbens
Symantec Corporation