Global Information Assurance Certification Paper

GIAC LevelOne - Internet Research Project

Cable Modems and Corporate Security

Ed Pardo
March 21, 2000

With the development of high-speed Internet access at home, there is an increasing migration of workers to home offices. This creates an interesting security dilemma. Now the corporate intranets are increasing in size one node at a time. The use of firewalls and perimeter defenses become more and more difficult to maintain. Are cable modems secure? What do I need to protect myself? Is it possible to securely work from a remote home office? These are a few of the questions that will need to be addressed by corporate information security staff. The rate of new subscribers is amazing. "CABLE DATACOM NEWS publisher Kinetic Strategies Inc. estimates North American MSOs pushed past the 2-million mark for cable modem customers in February 2000. U.S. cable operators counted an estimated 1.5 million installed cable modem customers at the end of February and Canadian operators served 560,000. Cable modem service was available to 43 million homes in the U.S. and Canada, equal to 40 percent of all cable homes passed. Kinetic Strategies estimates North American MSOs are now adding more than 5,000 new cable modem customers per day."[1]

When using a cable modem instead of a dialup connection, the benefit is a tremendous speed increase. Another benefit is that corporate programs that are IP based and web enabled like GroupWise and Exchange are now accessible at home. Connection occurs as if I am still connected to the company internal network with no noticeable decrease in speed. The down side is if the home pc is not configured correctly, I have just created a large hole in company security. The company policies must now extend to my home pc in order to protect corporate data. That statement has huge implications! Usually a network policy and a remote use policy are created but now, that distinction can get blurred. Fortunately, there are steps that can be taken to make the home pc a less likely target.

Most home pc's are win95/98 so the first step is to turn off file and print sharing. The next step would be to acquire a firewall solution. This could range from freeware or inexpensive software that runs in the background on the existing pc to a dedicated firewall appliance between the pc and the Internet. Products like Black Ice, Zone Alarm and WinGate are personal firewall solutions. Zone Alarm is freeware that is an application level firewall that lets you decide what uses the Internet. After testing it, I found it also

---

[1] Cable Datacom News MARCH 01, 2000. Kinetic Strategies, Inc. 20 March 2000. URL: http://www.cabledatacomnews.com/mar00/mar00-1.html

effectively hides ports and system information from the Internet. If NAT , multiple pc's, content filtering, or VPN support is required, a firewall appliance solution would be recommended. (Check with your ISP for what they will or won't support. My ISP doesn't support networks.) Companies such as SonicWall and Cisco produce firewalls for one pc/small networks that could be used depending on budget and features required.

I was curious to know what information was easily available from my pc so I set up Novell's LANalyzer. By capturing packets from my pc and analyzing them, I could determine what information was being transmitted and where the potential security leaks were. What I found was not surprising. Any website that was not using encryption, I was able to acquire username, password, email address, etc. from the captured packets. On the other hand, applications like Citrix that are encrypted make it very difficult to extract meaningful data from the packets. By allowing users access to the corporate network from home, policies need to be written to take this into account. If a users home pc is compromised and it has access into the corporate network, it would be hard for the firewall to detect that kind of intrusion. Instead of relying entirely on a firewall for security, the implementation of an intrusion detection system is recommended.

Now that the home pc is more secure, the corporate network needs to upgrade to an intrusion detection system.

"An intrusion detection system, or IDS for short, attempts to detect an intruder breaking into your system or a legitimate user misusing system resources. The IDS will run constantly on your system, working away in the background, and only notifying you when it detects something it considers suspicious or illegal. Whether you appreciate that notification depends on how well you've configured your intrusion detection system!

Note that there are two types of potential intruders:

Outside Intruders: Most people perceive the outside world to be the largest threat to their security. The media scare over "hackers" coming in over the Internet has only heightened this perception.

Inside Intruders: FBI studies have revealed that 80% of intrusions and attacks come from within organizations. Think about it - an insider knows the layout of your system, where the valuable data is and what security precautions are in place. "[2]

By adding another layer of security with an IDS and adjusting corporate policies, the migration of users to home offices can happen safely.

[2] COAST FEBRUARY 17, 2000. 21 March 2000. URL: http://www.cerias.purdue.edu/coast/intrusion-detection/introduction.html