Tech Talk

by Desmond Fuller

How Safe Is Your Computer System?

COMPUTER SECURITY has been getting a lot of attention lately. As companies and government agencies have made front-page news after being "hacked," they need to learn how to protect themselves and their employees from digital pirates.

Q: What is a hacker or cracker?

You might be wondering, "What kind of person would want to break into my system?" Unfortunately, that's a question most people ask after the intrusion has occurred. Most of the time, we refer to people that break into computers as "hackers" or "crackers." Originally, a hacker was what some computer people aspired to be. A *hack* means something that is created quickly to solve a problem (but not necessarily well).

Over time, the term has changed. Nowadays a "hacker" is someone that breaks into computers for various reasons. A cracker is someone that breaks security and is considered a "vandal" in the computer industry. Although they usually refer to themselves as "hackers," most are "crackers" and are common criminals that copy what other people have done.

Most hackers enjoy the intellectual challenge of circumventing or creatively overcoming a barrier. Some have done "cracking" in a playful way to learn various techniques but then have abandoned the practice.

Q: Why do they do it?

Sometimes it's an accident, other times it's the challenge, or it could simply be malicious. The sites that are most commonly hacked are high profile. Why? Because you can get more attention if you hack into the CIA than if you hack a small computer store. That doesn't mean that you're safe if you're not a well-known company. It means that large and more well-known companies are more at risk.

Q: What is a firewall?

Before it became a computer security term, a firewall was a structure designed to prevent fire from spreading from one location to another. In computerese, a firewall protects one network from another. The cost of a firewall can range from free to tens of thousands of dollars. This wide variance is due to different hardware, software, personnel, and consulting costs.

As Internet usage grows, firewalls are becoming increasingly important. That's because you are connecting your corporation's network to an "insecure" network—the Internet.

It's commonly thought that a firewall will solve all of a corporation's security problems. That's a dangerous misconception. A firewall establishes a "perimeter defense," which is similar to a moat surrounding a castle, but there are other considerations such as inside attacks, viruses, and modem lines.

Typically, there are two types of firewalls: packet filtering and application gateway. In the first type, filters "tell" the firewall what kind of traffic to allow in and where it should go. For example, a filter might let users from company.com enter and log onto a computer, but users from school.edu would be filtered out. This is a very simple example, but as a network gets more complex, weaknesses crop up. The more filters, the more mistakes. And that means that the wrong traffic may get into your network.

With an application gateway firewall, you can have more flexible and tighter security. It uses proxies, which are programs that act as "bouncers" at the corporate network's entrance. For example, if a user logs on to a proxy, it can document what that person is doing, who he or she is, when he or she logged in, and where he or she will go. At that point, the proxy can authenticate the user (with a password or the originating location) and allow the user in.

The problem with that type of firewall is that it requires more work to log onto the system or may require special programs to use it.

Both types of firewalls can be used together. Each has its weaknesses and strengths, and by combining the two you can get a more efficient hybrid.

Q: What can companies and individuals do to protect themselves from hackers and online piracy?

A firewall is the first step, but there are other precautions that a company can take.

The most commonly missed security problem is a failure to look at human factors. For example, are passwords, such as a spouse's name or your child's name, easy to guess? Are passwords rarely changed? Is confidential information (including passwords) left in the open? Almost 50 percent of most intrusions are from insiders and could be avoided easily by simple password policies. Here are a few suggestions:

- Use nonletter characters.
- Use at least six characters.
- Don't use the names of your spouse, kids, or pets.
- Don't use a word found in a dictionary.

Computer viruses are another common problem. They are programs that embed themselves in other programs or documents. Viruses do different things such as put a picture or words on a computer screen or erase a hard drive. Some of the newer firewalls can scan for viruses, but they are not foolproof.

Most viruses still come from floppy disks, which have not been virus-checked before use. A dedicated virus-protection program on your computers and network, as well as antivirus policies, can provide a complete solution. Two well-regarded antivirus packages are McAfee Associates' Anti-Virus, http://www.mcafee.com, and Symantec's Norton AntiVirus. (Networked and PC versions are available.)

Just because policies are in place and firewalls are installed doesn't mean an organization can forget about security.

Network administrators should perform tasks daily to protect a network. They should check periodically for known security issues and patches (programs that fix bugs) on WWW servers, FTP servers, routers, and operating systems. Administrators should look at server logs daily. Take a snapshot of a typical day on your network. With this baseline, you can tell if something strange is going on.

Also, use security programs to sweep your network for possible weak links such as unsecured passwords or machines that have not been secured correctly. For example, Crack, password cracker software, should be run periodically on your system. If it can't crack your passwords, it's unlikely that someone else using the same program will be able to.

Copyright protection

In addition to network security, companies must be able to protect copyrights such as company logos, software programs, and intellectual property on the Internet.

Recently, the Clinton Administration proposed rewriting various copyright laws to protect content creators on the Internet. It presented the "Database Investment and Intellectual Property Antipiracy Act of 1996" to Congress.

The United States and other delegates from 18 other countries in the United Nation's World Intellectual Property Organization have also met to revise existing international copyright regulations.

One protective technique, a digital watermark, is similar to the watermarks that are imbedded in high-priced stationary. Digital watermarks insert identification such as a company's logo and copyright data into an image or document. It can help a company prove that the image or document was copied illegally. IBM Research and NEC Research Institute have studied this technology extensively. Two other companies, the DICE Company, http://www.digital-watermark.com, and the Digimarc Corporation, http://www.digimarc.com, offer digital watermark products and information.

Distribution of software over the Internet is another problem. Some software companies are experimenting with encrypted envelopes, which are used to send copies of computer programs to potential customers. A user on the receiving end needs a digital "key" to open the envelope. This method lets software publishers quickly distribute software programs without worrying about illegal copying.

One popular software program, PGP (Pretty Good Privacy), can be downloaded for free at http://web.mit.edu/network/pgp.html. It lets you send encrypted e-mail that can only be read by designated people.

Even if you use privacy software to send e-mail, it's still a good idea to stick to this advice from the experts: Don't write an e-mail that you would not feel comfortable seeing on a public bulletin board. ■

Desmond S. Fuller *is cofounder of Pencom Systems Administration. He can be reached at 1801 Alexander Bell Drive, Reston, VA 20291. Phone 703/860-2222, e-mail desmond@pencom.com.*