Enemies from without and within are constantly looking for ways to break into vulnerable computer systems. All it takes is one successful attack to bring down an entire system. PREVENTING COMPUTER FRAUD

By Greg Hanna

COMPUTER FRAUD IS A BOOMING BUSINESS. Only a small percentage of computer criminals are ever apprehended, and even when they are caught, the courts tend to treat them leniently. Maybe that's why there are so many hackers and crackers out there trying to break into or bring down computer systems. They don't fear being called to account.

Corporate America has shown a surprising reluctance to bring these criminals to justice. The *2004 Computer Crime and Security Survey* by the Computer Security Institute and Federal Bureau of Investigation found that the percentage of organizations reporting computer intrusions to law enforcement is actually declining, with fewer than half reporting such intrusions. The key reason cited for not reporting intrusions is fear of negative publicity. Many of the computer crimes that are reported expose embarrassing breaches in computer security.

How big is the problem? Studies show that small companies are subject to several attacks every day and that giant corporations are under attack virtually every minute of the day. The vast majority of these are virus attacks, most of which are repelled.

All too often, human failure, like giving your password to another person, creates the opportunity for fraud.

Yet despite their numbers and persistence, these outside hackers and crackers are just a small part of the story. The greater danger comes from within. A widely quoted figure claims that 75% of computer crimes are committed by insiders.

Often it's difficult to spot the culprits. In one company, an assistant to the CFO lent her password to a colleague. That colleague subsequently used the assistant's computer to access the system and make unauthorized payments to two dummy corporations. Suspicion fell upon the CFO's assistant. Fortunately for her, a thorough investigation uncovered the conspiracy and exposed the real thief. In this case, the company reported the crime to law enforcement, and the thief was tried and convicted of fraud.

The real failure lay with the company for not keeping a tighter grip on its password security. All too often, human failure, like giving your password to another person, creates the opportunity for fraud. Training can greatly reduce failings like this, but all it takes is one mistake to leave the system open to attack. In addition to training, then, companies need to build strong defenses around their systems. It's a lot cheaper to keep intruders out than to clean up after them.

GUARDING THE PERIMETER

Let's take a look at the first line of defenses.

Firewalls. An effective security system protects a company's computer operations with a series of defenses, like the walls and breastworks around a fort. The intruder who slips past the first line of defenses runs into another and then another and another. Usually, they get frustrated and quit.

The initial perimeter defenses are the firewalls. A firewall is like a steel-reinforced concrete fence with a few well-chosen gates. A small company may have a single firewall. A giant corporation may have firewalls on every floor and around every department.

Some people think of firewalls as the toughest defenses. Actually, they may be among the weakest. Firewalls limit external access to designated gateways but do little to protect the network from people who are already inside—disgruntled employees, would-be thieves, vandals, and the like.

In setting up firewalls, administrators try to build barriers that are strong enough to keep out would-be intruders but not so impermeable as to make it difficult for legitimate users to move information over the system. To meet these conflicting demands, the administrators have to make some compromises. As a result, many firewalls have undetected vulnerabilities that hackers can exploit.

To protect system integrity, some companies use vulnerability-scanning tools that continuously examine the system for oversights and vulnerabilities. These tools can monitor for a wide range of irregularities, including unauthorized software, unauthorized accounts, unprotected logins, weak passwords, and inappropriate access permissions.

Authentication. Getting through the firewall and gaining access to the system typically requires authentication in the form of a login name and a password. Bad and poorly guarded passwords are the bane of most systems. Users typically use four- to six-letter passwords, often words or dates that are easy to remember. With current technology, a hacker can crack a four-letter lower-case password in less than a minute and a six-letter lower-case password in less than an hour. If the password is an everyday word, even a long one or one written backwards, a hacker can easily crack it with an "online dictionary" attack, which can run through an entire English or foreign language dictionary, backwards and forwards, in a matter of minutes.

To deter intruders from guessing passwords, a password should have at least eight characters, including numbers, symbols, and both upper- and lower-case letters. As an added precaution, the password should be changed at frequent intervals, with the system automatically alerting the user when it's time to change.

Unfortunately, many users make it easy for intruders to steal their passwords. Because complex passwords are hard to remember people often jot them down on a slip of paper and tuck it away under their keyboard or even post it to the frame of the computer. Also, users are often tricked out of their password. They get a phone call from "MIS" saying there's a problem with their access to the system. The voice asks, "What password are you using?" And the unsuspecting employee gives away the password and unwittingly opens the system to the hacker.

In the course of an ordinary day, a large corporation's perimeter may be attacked by tens of thousands of scans, probes, pings, and viruses.

A more insidious approach is called "spoofing." The spoofer makes the user think that he or she is talking to the system and, in that way, steals the password or other security information. For example, the spoofer may display what looks like the system login prompt on a terminal to make that terminal look idle. When the unsuspecting user logs in, the spoofer gets both the login name and the password. After getting this information, the spoofer prompts the user to try again. The user then logs on again, never suspecting that he or she has been victimized.

A "secure attention key" can prevent this kind of spoofing. When a user hits the key, it kills any process

HOW MUCH PREVENTION IS ENOUGH?

How much should a company invest in system security? It depends on the amount of risk. Small manufacturers with no valuable trade secrets might make do with inexpensive systems that protect such things as accounts receivable, payroll, purchasing, and supplier payments. But large financial institutions with billions of dollars under their care will need far more sophisticated security systems that, in effect, create layer upon layer of security.

Going overboard on security can waste money and hinder operations. For example, too complex a system can cut into employee productivity.

To find the right balance, a company can create fraud and theft scenarios and then develop a security system that will hold potential losses to an acceptable level rather than trying to eliminate losses altogether. In other words, there's a point at which the cost of additional security will outrun the potential losses.

running at the terminal and guarantees a trusted path to the system.

Fighting Viruses. In the course of an ordinary day, a large corporation's perimeter may be attacked by tens of thousands of scans, probes, pings, and viruses. The firewalls will deflect the vast majority of them, and most of those that sneak through will be stopped by anti-virus software. Because new viruses are constantly being unleashed, this anti-virus software must be updated regularly with the latest "signature" files telling the anti-virus software what to look for.

The final line of defense is the computer user, who should be trained to recognize and reject suspicious e-mails. Unfortunately, employees are all too often tricked into unleashing viruses. They receive an e-mail that seems to come from a colleague, client, or customer and promptly try to open the attachment, usually one with an .exe, .bat, .scr, .zip, or .pif file extension. The virus is then loosed into the system.

Rather than risk leaving it to employees to recognize and delete suspicious e-mail, many companies use anti-spam systems to capture or kill virus-infected spam before it can reach anyone's PC. That minimizes the human element from the risk equation.

PROTECTING THE CORE

Now let's go a little deeper.

Anti-Spyware. Spyware is tracking software that sneaks into the user's computer, often bundled with legitimate software, and then reports back to the "mother ship" on the user's computer activities. For example, it can monitor every keystroke and, in that way, enable crackers to steal credit card and other financial information. It can also hijack the company's system and use it for other purposes, such as storing and transmitting pornography.

A number of anti-spyware software products (Spy Sweeper, Spyware Eliminator, AntiSpy, SpySubtract) can identify spyware and other hidden programs, such as Trojan Horses, and remove them. A Trojan Horse is defined as a "malicious, security-breaking program that is disguised as something benign." For instance, the user may download what looks like a free game. Then when the user tries to run the "game," the program erases every file in the directory.

Network World recently reported on a piece of spyware that disabled the security controls on a forensic investigator's browser and took control of it. Every time the investigator tried to erase the programs and reboot the machine, the software reinstalled. Eventually he was able to remove it using a remediation kit.

Most wireless access points are unprotected, leaving the corporate network vulnerable to attack or misuse.

This investigator's distress shows how sophisticated hackers and crackers are becoming. If they get a toehold, they can take over the entire system.

Making Wireless Safe. The popularity of wireless laptops, notebooks, and PDAs has created a whole new threat to corporate computer systems. The problem is that the wireless access ports transmit continuous radio signals. Armed with just a laptop, a wireless adapter, and wireless scanning software, a hacker can park near a company and pick up these radio signals. If the system isn't protected by a secure password, the hacker can break into the wireless unit and from there gain access to the company's computer system.

There are a relatively small number of vendors of wireless network adapters, each with a limited number of default user names. Since very few wireless users bother to change the default name to a secure code, most wireless access points are unprotected, leaving the corporate network vulnerable to attack or misuse. One solution is to have every wireless user change the default name to a secure code. But if just one person fails to take such a step, the system will be wide open. For this reason, many companies have installed Wireless VPN (Virtual Private Network) Access Points.

A Wireless VPN Access Point grants access to the system to wireless users only if they are properly authenticated by a "custom generated" encryption key. Scanners can still detect the presence of a wireless network but can't get into it without a verifiable encryption key for that specific unit and Wireless Access Point.

With VPNs, the password or software authentication code can be the weak link. For this reason, some companies give their employees "authentication tokens." One kind of token looks like a key fob with a string of LCD numbers. To get into the system, the user enters the number on the token. To make this approach almost unbreakable, every employee has a different number, and the individual numbers change every few minutes in synch with the master server at the company's office.

Server Locking. Despite all the precautions, most systems are still vulnerable. That's because systems in both large and small companies require administrator or super-user-level passwords for system maintenance, repair, and upgrades, and these passwords are bound to get out.

To deal with this threat, some companies use server-locking software that, in effect, builds an encasement around the operating system's kernel. The kernel is the essential center of a computer operating system, the core that provides basic services for all other parts of the system. Encasing the kernel doesn't affect everyday users at the outer periphery, but, via the keyboard directly attached to the servers, it does prevent anyone from gaining unauthorized access to the very core of the system.

To get past this encasement requires a password that is held by just one person and is changed regularly. Before an IT engineer can work on the kernel, the password holder has to grant access. Only then can the engineer log in, even as the server administrator.

INTRUSION DETECTION

Building a completely secure system isn't feasible. For this reason, many defense systems include intrusion detection. Detecting breaches in the system provides information for eliminating flaws and tracking down crooks. If a person tries to break through the firewall and into the system, a "trigger" is tripped, and now the system watches this person's activities, logging everything as that person moves through the network, like a fox chasing a rabbit. Because every Internet connection has an IP (Internet Protocol) address linked to it, forensics experts can use the intruder's trail to backtrack to his or her site.

One company allowed its salespeople to have FTP (file transfer protocol) capabilities. FTP is simply a method of transferring files over the Internet. A salesman who was planning to leave the company and join a competitor set up his home computer as an FTP server and then stole the company's entire database by transferring it to his home via FTP. Fortunately, the system kept a detailed log of everything he did, and forensics was quickly on top of him.

In this case, the company made the serious mistake of giving employees capabilities, like FTP, that weren't necessary for their work.

AN OUNCE OF PREVENTION

Cleaning up after an intrusion can be incredibly expensive, so it's critical to prevent intruders from gaining access or, if they do slip in, to limit their range and the damage they can cause. In terms of preventing fraud, here are several points to keep in mind:

◆ Create a security policy that clearly spells out what to do in the event of attack and who has the authority to pull the plug on the system.

◆ Establish specific responses for dealing with different kinds of intrusion threats. The plan should be preapproved by the CEO because it will be too late during an attack to get such approval.

◆ Establish both internal and external communications guidelines. How and when do you notify vendors and customers that their systems may have been compromised? Do you report the intrusion to the police or FBI?

◆ Ensure that everyone knows how to contact MIS if they suspect a system has been compromised.

◆ Set policies regarding access, passwords, and authorization—and enforce them.

◆ Scan the system regularly for anomalies, weaknesses, unauthorized usage, and other signs of misuse.

If you follow these procedures, you will have an excellent chance of keeping your computer system safe. ■

Gregory Hanna is founder, president, and CEO of TOSS Corporation (www.DisasterAvoidance.com), which has been providing security, network, and disaster avoidance services since 1992. You can reach him at (888) 884-8677 or at LegalData@DisasterAvoidance.com.