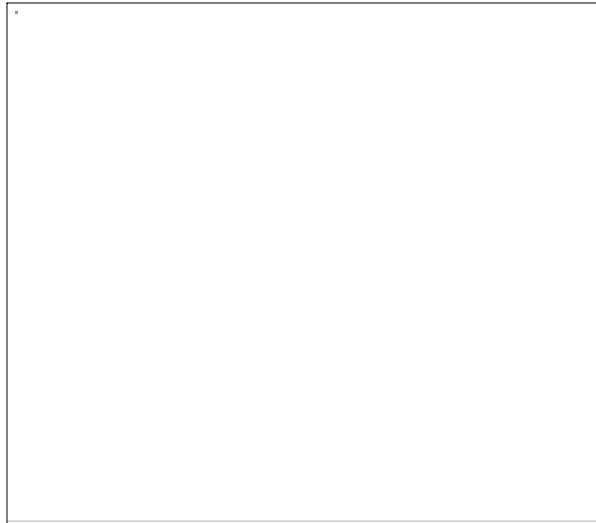


Is Your Network Safe?

Attacks against Microsoft underscore the dangers facing the computers of corporate America

Even Microsoft is vulnerable to network break-ins, sparking worry among other digital corporations



By Erik Sherman
NEWSWEEK

Nov. 27 issue — Feel sorry for Microsoft? Who would've thought it? Yet it's hard not to have at least some sympathy for the software giant lately. In October someone broke into its network and rummaged around for almost two weeks, sending valuable product source code to Russia.

Figures from an annual joint study of the Computer Security Institute and the FBI suggest that 42 percent of the 643 respondents had total financial losses of \$265 million

DAYS LATER, A DUTCH hacker exploited a software flaw in a Web server in order to gain access to one of Microsoft's machines.

Still, security experts say that Microsoft has top people heading its internal-security efforts and the resources available to do the work right. If it can get caught so flat-footed, most companies seem like sitting ducks. It's one of the biggest worries of corporate America these days. In fact, figures from an annual joint study of the Computer Security Institute and the FBI suggest that 42 percent of the 643 respondents had total financial losses of \$265 million (ranging from the loss of revenue when servers were down to the expense of fixing sabotaged systems). "That's close to \$1 million [each]," says Kae Lovaas, vice president of technology underwriting at the St. Paul Cos., Inc. Critics say the CSI-FBI study is inaccurate. But no one

suggests businesses can relax. Many security breaches are never revealed by their victims because they fear bad press.

Some attacks on corporate systems are done by amateurs like the Canadian youth who brought down Amazon.com and CNN.com last February. They're called "script kiddies," for the practice of downloading any of the hundreds of software programs available for finding passwords, attacking servers and probing defenses. What made the first Microsoft attack unusual was its criminal nature; the perpetrators were looking to steal something of value. Such people are far more skilled, and dangerous, than script kiddies. "If we know about it, it probably wasn't [a professional attack]," says John Woodward, director of information warfare at the MITRE Corp. "Essentially they come in under the radar and over a period of time build up knowledge of a target." George Kurtz, CEO of Irvine, Calif., security-consulting firm Foundstone, Inc., remembers a big telecommunications company that had an intruder on its systems for at least six months before his firm was called in. "They had access to just about every system on the network, including the firewall," Kurtz says.

Corporate managers often don't realize how vulnerable they are. In April 1999, KPIX, a CBS TV station in San Francisco, found that someone had managed to get into its Web server, lock out the staff and put up faked stories. The station secured the point of entry, but then found itself compromised again when someone brought the Web server down and, with it, advertising revenue. "[The cost] must have been a few thousand dollars each day, and it was down for a few days," says Webmaster John LeBlanc, who started working at KPIX after the second attack. The company took steps, including deploying a firewall from AXENT Technologies. But it can sometimes be difficult to get management to spend money on proper security tools and personnel before the company becomes a victim.

Given the price of security, it's easy to see why. Implementing thorough computer security in a Fortune 500 company, including experienced personnel and specialized software and hardware, can run \$15 million to \$20

Ten Steps to Better Security

Where's the weakest link in your security chain? Maybe it's you. Ten things to think about:

- 1. You'd be surprised how many employees write their passwords on sticky notes, and put them on their monitors. The security-conscious stick

million, according to some estimates.

Companies in the \$100 million to \$500 million range would likely spend more than \$2 million. Small companies that outsource most security needs should expect to spend between \$100,000 and \$200,000.

Money alone, however, doesn't guarantee good security. The most important step is to balance risks against costs. "Most people don't go through the process of determining how valuable the data is... and is that number greater than, equal to or less than what it costs to protect it," says Fred Rica of Price Waterhouse Coopers'

the notes under their mouse pads.

- 2. Companies throw out sensitive material without shredding it. If a thief can raid your trash for a print-out from your database, why bother hacking?
- 3. How much physical security do you have? In many places, anyone with a pizza box can walk in, get what's needed and walk out.
- 4. Almost no one does a background check on programmers. Even fewer ask about the people working for the nighttime cleaning service.
- 5. Firewalls and other forms of security software can be hard to configure. One wrong turn, and there's an open door to your network.
- 6. Every operating system has default passwords set by manufacturers, so administrators can get in for the first time. That means everyone knows them. Did you change yours yet?
- 7. Outsiders can access your network if you allow dial-up modems at employees' desks. All they need is the phone number. And don't put too much confidence in passwords: there are cracking programs that find passwords through brute computing force and a knowledge of tricks, like substituting the number 1 for the letter l, that users think keep them safe.
- 8. Some computers are more valuable than others --like servers, for example. Are yours behind locked doors?

- 9. Your system management tools have security logs and both network and host security-monitoring programs. If you don't review them daily, you'll miss evidence that can warn you of a current attack. Some monitoring software will also send alerts.
- 10. Train your employees on procedures that might keep intruders out. For example, don't let employees set their e-mail to automatically open attachments, which might carry viruses or Trojan horses.

technology-risk-services group. In his opinion, many managers make decisions on “conjecture.”

Even with the best of plans, security can fall apart because of the human factor. Training alone can't guarantee that people won't err. Jim Geary, CEO of SHYM Technology, which makes security tools for applications, brings up what happened to him in May with a computer virus. “I got an iloveyou message from the chairman of one of the public information-security companies,” says Geary. “This is a chairman who's been in the business for 10 years. Even some of the people who should have had their systems set up with the proper security didn't.”

In a way, the focus of news stories on computer break-ins from the outside can lull companies into ignoring the more important internal threat. The 7-Eleven store chain recently discovered that last May an employee had found a way into the e-mail box of “a fairly high-level senior executive,” according to chief information-security officer Todd Cohen. The employee wasn't malicious, just curious, but that doesn't help a company with information set loose.

When an employee is looking to cause damage, the problems are bigger. “The average outside hack costs a company about \$56,000, and the average inside job costs a company about \$2.7 million,” says Richard Isaacs, senior vice president of the LUBRINCO Group. Often companies make sabotage or theft easy by not removing the network accounts of former employees or by failing to shred documents.

If threats from disgruntled employees weren't

enough, companies must also consider cyber terrorism. Organizations that might have kidnapped someone in the past are finding that nabbing a corporation's computers might be more effective. The Internet itself is vulnerable because, even though traffic can be routed in different ways, there are high-capacity points. "Until two years ago, over 50 percent of Internet traffic was routing over [one] Internet exchange," says Amit Yoran, CEO of the network-security-monitoring firm Riptech.

The future is worrisome. As the technology to foil break-ins becomes more sophisticated, so do the rogues on the other side. "It's always a cat-and-mouse game," says Pete Tasker, director of security and information operations at MITRE. The digital detective work is just beginning.