

September 15, 2004

Cybercrime

How to stay safe in the chaos of cyberspace

Within the last three months, U.S. law enforcement agencies have conducted a wide-ranging “sweep” of criminal activity on the Internet, with more than 150 people arrested, charged or convicted as a result of investigations. The cases, involving credit card fraud, corporate espionage and other offenses, produced losses in excess of \$215 million.

The international threat of cybercrime poses a serious security concern to individuals and corporations alike. As in the security of facilities, business leaders must take a broad view of security involving proprietary information and electronic assets. In fact, a keen focus on securing information technology (IT) may soon become more than just an advisable business tactic—the Securities and Exchange Commission (SEC) and other federal regulatory organizations are evaluating proposed legislation to require enhanced security measures, such as companies filing statements attesting to IT-security readiness.

In this issue of The Lipman Report, Richard Clarke, former Cyberspace Security Advisor to the president, offers recommendations for protecting computer systems both in the workplace and at home.

Current Threats

The computer security landscape continually evolves, in many cases faster than security professionals can respond. As businesses first brought commerce to the Internet, the threat was compromised data; it was passed in the clear and easily intercepted. Cryptographic solutions dating back to the late 1970s provided solutions that resulted in Secure Sockets Layer (SSL) connections. Now, anyone can shop at online retailers and exchange information that only the shopper and retailer can see, but even these security solutions are under attack. For example, one tool used allows a third party to capture keystrokes typed on a computer. That information entered by the user can be easily captured in the clear and forwarded for storage and possible illegal use.

Threats from nation-state entities and organized criminal enterprises cannot be ignored, but in the end, they typically access systems through the same vulnerabilities other criminals do.

Implementing stringent security policies and managing vulnerabilities as they are discovered can protect a system against most threats. Continuously strive to understand and adapt to evolving threats, while focusing on securing vulnerabilities before they are exploited.

Criminal activity against Internet users has increased substantially over the years. Although there is very little solid scientific data on the extent of this activity, the U.S. Secret Service and Carnegie Mellon University’s Software Engineering Institute learned in a survey that 70 percent of respondents report at least one criminal intrusion against their organization. These respondents estimated that such activities cost them approximately \$666 million in 2003. Those that could identify the threat found 71 percent came from outside, with 29 percent from inside.

The SANS (SysAdmin, Audit, Network, Security) Internet Storm Center tracks the top-10 ports for attack activity. This ever-changing list provides a good point of reference to understand the general threat across the Internet and provides pointers when exploits are blossoming. During the week of August 23, 2004, for example, SANS listed two Trojan worms, two NETBIOS attacks, two Microsoft SQL Server attacks, and the MyDoom virus.

Companies cannot wait for government measures to improve computer security. The private sector ultimately holds responsibility for protecting its IT systems, and businesses must take action now, before disaster strikes. Effective IT security also plays an integral role in a company’s compliance with the Sarbanes-Oxley Act of 2002 by protecting the company’s financial reporting system and proprietary information, loss of which could have a demonstrable impact on company financial statements.

Since threats continuously adapt to established security measures, what constitutes effective practices today will be old hat tomorrow. IT security has become a process of continuous change, policy review and awareness.

(continued on next page)

Cybercrime

How to stay safe in the chaos of cyberspace

(continued from preceding page)

The Corporate Network

Advanced technology continues to provide global business opportunities, productivity gains and increased convenience. At the same time, reliance on technology creates enticing opportunities for exploitation by thieves, disgruntled workers and terrorist agents. A proactive approach to computer security can yield tremendous benefits in protecting information and ensuring business survival.

Make security a priority. Ensure that computer security is a concern at the executive level, and incorporate security as a performance tool in evaluating the IT department's effectiveness. Consider implementing procedures to evaluate the transmission of information to ensure employee compliance with established guidelines.

Encrypt. One way to secure information in storage and in transit is through encryption. Encryption can be applied to individual files, storage drives and messages, with access to decrypt granted to customers and clients. If hackers can get into a system through other vulnerabilities, they cannot read encrypted data provided a strong, testing cryptographic algorithm has been used. Advanced Encryption Standard (AES) is the suggested standard (128-bit key size). The National Institute of Standards and Technology (NIST) provides guidance on cryptographic solutions and uses.

Stop the insider threat. Prevent employees from creating e-mails that could embarrass the company in court or reveal corporate secrets by using egress and content filtering software. Compartmentalize the network into "need to know" islands with access control lists, so employees in accounting cannot look at the latest discovery by the research and development department. Use awareness tools to educate staff about the seriousness of Internet security and common mistakes such as a password under the mouse pad or using a disk brought from home. Organizations need to create and enforce policy for the use of portable hard drives, which

provide not only greater mobility, but also increased risk of misuse or file corruption. Critical proprietary information can easily be stored and removed undetected from a facility using a drive no larger than a lighter.

Automate. Constantly scan the network with automated audit software to know what systems are connected and whether any devices have unremediated vulnerabilities. Similar software can enforce security policy rules (e.g. no unauthorized wireless devices linked to the network). After examining a system, automatically update the anti-virus definitions installed.

Reign in the road warrior. Employees on the road connect back into the corporate network over secure Virtual Private Network connections that can inject worms and viruses from insecure laptops, opening the internal network to infection. Prevent this common source of compromise by using software that interrogates the remote device based on a security policy before completing the connection to the network.

Secure user identity. If simple passwords are used to authenticate users, then a hacker can access a network within minutes. Enforcing strict password rules and using at least two-factor authentication, combined with Identity Access Management software, will prevent hackers from pretending to be employees or clients. The key lies in ensuring that internal users, as well as outside users, are who they claim to be.

Stay informed. Use the capabilities of open-source intelligence services that have demonstrated the ability to warn of a worm or virus before it hits. Free resources, like the SANS Internet Storm Center and US-CERT (United States Computer Emergency Readiness Team), can provide warnings and vulnerability announcements. These services may communicate what software updates, or "patches," are urgent or recommend ways to "work around" and provide router and firewall rules until patches can be applied.

Join up. Join an industry Information Sharing and Analysis Center (ISAC), the U.S. Secret Service's Electronic Crime Task Force, or the Federal Bureau of Investigation's regional Infraguard. The local chapter of the Information Systems Security Association (ISSA) may also be useful for a company's IT staff. Investigators on staff should participate in organizations such as the High Technology Crime Investigation Association (HTCIA).

Keep public Web pages off network. Prevent hackers from entering the network through public Web pages by keeping such pages (including interactive ordering forms) off the company's network, and instead cached on a providers' network of secure servers. If the organization relies on such pages for commerce, many caching services can also provide uninterrupted access regardless of traffic load through globally deployed servers.

Utilize outside experts. An IT staff alone cannot always provide timely response around-the-clock to manage the system's Intrusion Detection Systems (IDS) and firewalls. Outsource that role to a reliable security service provider. Enlist an Internet service provider (ISP) that can perform security tasks that the company would otherwise have to do to prevent spam, worms, viruses and denial of service attacks.

Protect both the network and the desktop. Don't decide whether to place the firewall and anti-virus software on the network server or on desktops; do both, with personal firewalls and anti-virus programs at client locations in case something penetrates the network's edge defenses.

Secure all software. The most recent software purchased (or specialized software custom-made for the company) has mistakes in it that a hacker will find someday. Buy software that checks other software for vulnerabilities. In addition, consider diversifying to less widely used software, which removes a system from the larger target space.

Finally, realize that no matter how rigorously a company implements and enforces security pro-

cedures, its data or network may be compromised. Always have a plan for recovery and restoration, along with the software to do it, and test the plan at least twice a year.

The Home Computer

The home computer is just as critical to secure as a corporate network; all are participants on a global network. Many home computers are compromised to become unwitting participants in zombie networks that attack others. Everyone should do his or her part to practice good hygiene so as not to become one of these participants. A legal concept called "down-stream liability" is beginning to grow in use and may provide further legal incentive for individuals to follow suggested practices.

Install a firewall. Anyone who has used a broadband connection without personal firewall software installed has probably already had his or her computer penetrated. Purchase, install and continually update personal firewall software online or at the electronics store. A recent study found that unpatched, unprotected PCs are compromised within 20 minutes of connecting to the Internet.

Keep anti-virus software up-to-date. Anti-virus programs that come with computers are out of date by the time buyers first use them. Subscribe to an automatic update service and maintain a subscription to the service. Anti-virus signatures can be updated multiple times per day. If an anti-virus program does not have the latest definitions, it cannot detect all of the malicious code hitting the computer's system. Systems should be set up to check daily for updates.

Change the password. A user's password should be at least eight digits and employ numbers, upper and lower case letters, and symbols. The user should change his or her password every three to six months, or each time there is a possibility that the system may have been compromised.

(continued on next page)

Cybercrime

How to stay safe in the chaos of cyberspace

(continued from preceding page)

Change the screen name or use two. Prevent spam and other nefarious activity by changing each user's screen name every year. Or at least log in to a second screen name before surfing the Web: one screen name for sending and receiving e-mail, another when looking at the Internet. Most Internet security software packages also include a privacy monitor and anti-spam utility. These should run at all times to help prevent the unauthorized passing of private information.

Update the operating system. Check regularly with the software company that made the computer's operating system to get security patches, or use an automatic update feature. This process should be done in addition to anti-virus updates.

Watch for spyware. Some Web sites have been infected with spyware that drops into a computer and monitors the user's keystrokes for passwords, credit card numbers or other activity. Buy and run anti-spyware software, in addition to anti-virus and firewall software.

Turn things off. By default, a computer may be set up for file sharing and instant messaging and other services. Turn settings like this off except when needing to use them.

Do not use wireless networks without protection. Unless a computer user lives on five acres of land, he or she should not use wireless home networks without encrypting. This process can be complicated, so expert help may be needed.

Use caution when buying online. If using a credit card online, use one from a bank that will provide software that generates a new number for each transaction. These "one-time use" numbers are safe, even if compromised. If a warning is issued about the site's security certificate, pay attention to the warning. It is important to remember that calling a company's 800 number may be no different than placing an order online. The information provided is stored in the same place. Banks used to practice a policy of knowing

their customers, and it is a safe policy for purchasers to practice, too: know the merchant. The best price may not always be the best purchase.

Employ enhanced security when banking or trading online. Anyone with a lot of money in an account should not just log into the site with a password. Ask the bank or brokerage house for a "secure token," another layer of identity confirmation. They usually give this added security to highly valued customers—and to those who ask.

Diversify. Internet browsers that are widely used are more likely to be employed by hackers to attack than the less well known. The same is true of operating systems and commonly used applications.

Choose a trusted Internet service provider. Some ISPs try actively to prevent fraud, worms, viruses and spam. Ask if they do before selecting an ISP. Also, never succumb to "phishing," which is an e-mail that looks like it comes from an ISP, bank, credit card company or broker asking the user to follow a link to update billing or credit card information. Regardless of how legitimate a request appears, do not respond via e-mail. Instead, call the sender of the message to verify that the information is needed.

The sophistication of computer technology offers boundless possibilities for business and personal use. Taking advantage of these advancements, however, presents myriad risks, from mischievous pranks to devastating theft. By taking protective measures and constantly improving those procedures, corporations and individuals can improve security in cyberspace.



The Lipman Report Editors