Your 10 Biggest Network Security Worries

The right hardware, policies and user education can help in the fight.

From spyware and phishing to intrusion attempts, the threats attacking today's computer networks are more dangerous than ever. Many threats are targeting specific industries with convincing-looking e-mail and phone calls. The hackers hope to direct employees to counterfeit Web sites, in order to harvest passwords and private financial information or steal computer and network resources. "The revenue from cybercrime in the United States now exceeds that of illegal drug activity," says Scott Pinzon, editor-in-chief of WatchGuard's LiveSecurity Service, WatchGuard Technologies Inc.

"We're seeing a change in the threat landscape, from ones that were noisy and targeting the perimeter of the network, to becoming much more silent, difficult to detect and highly targeted," says Kelly Martin, group product manager, Symantec Corp. "These attacks are mostly targeting Web browsers and the client applications on the computer itself. And while a small business network may not be as complicated as an enterprise network, they still have desktop and mobile clients."

Because small businesses have fewer IT resources at their disposal, they need solutions that provide comparable protection, at affordable costs and requiring minimal administration. Here is a list of the biggest threats or sources of vulnerabilities today's small business IT professionals need to defend their networks against, along with tips on how to fight them.

1 Spyware

Spyware is software that installs itself on a computer without the knowledge or permission of the owner, be it your company or the main person using the system. According to antispyware vendor Webroot Software Inc.'s State of Spyware Report, nine out of 10 PCs connected to the Internet are infected with spyware, and some form of spyware can be found on 87 percent of corporate PCs.

Spyware can get into your computer from executable attachments in e-mail, "hostile applets" on Web sites, hidden on installation CDs or downloaded files and through security holes in other applications. Spyware also "piggybacks" on top of quasi-legitimate downloads, often pretending to be a browser accessory or important security update. Sometimes the "permission" is buried in the fine print of an end-user license agreement (EULA) document or Web page.

Once installed, spyware programs often masquerade as legitimate files or programs, or do other tricks to avoid detection. Some spyware may simply attempt to change your browser's home page or present pop-up ads. Too much spyware — even of this type — can seriously degrade a computer's performance, increasing startup and shutdown times, slowing regular operations to a crawl or bringing the machine to a complete halt. But increasingly, most spyware is malicious in intent, monitoring a user's keystrokes or examining their files for passwords, financial account numbers and other sensitive data, and then sending that information back to the spyware's creator, who may use it for identify theft.

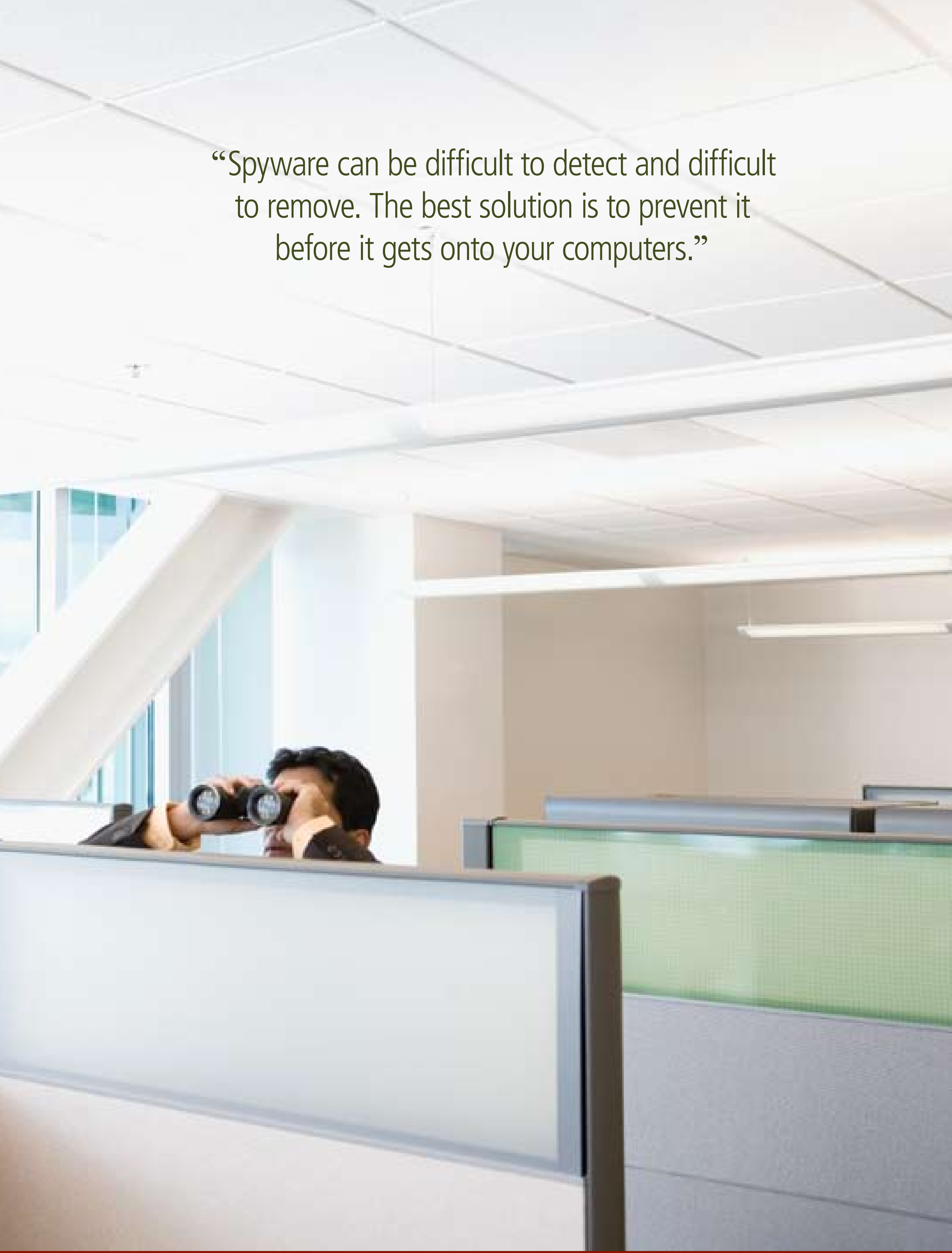
Spyware can be difficult to detect and difficult to remove. The best solution is to prevent it before it gets onto your computers, by doing URL (Uniform Resource Locator) and content filtering at the network gateway and, if possible, on the computer. However, it's also important to run antispyware software on user machines, such as McAfee AntiSpyware, Trend Micro Anti-Spyware and Webroot Spy Sweeper. For a hardware solution, consider Barracuda Networks' Barracuda Web Filter, previously known as the Barracuda Spyware Firewall. The Barracuda Web Filter attacks existing spyware installations by detecting any spyware access to the Internet and notifying the administrator.

2 Blended Attacks

As the name suggests, blended attacks combine several types of activity. They combine the characteristics of viruses, worms and other malicious code with server and Internet vulnerabilities to rapidly initiate, transmit, spread and cause widespread damage.

"The goal is to extract confidential information from your system," says Symantec's Martin. "It may start with a phishing attack through e-mail, instant messaging »

“Spyware can be difficult to detect and difficult to remove. The best solution is to prevent it before it gets onto your computers.”



[IM] or a 'voice phishing' call as the point of entry, figuring out how to get your attention." Then the attack tries to trick the user into going to a Web site that drops malicious code, so even if the user doesn't give private information, their system gets compromised.

Tools to block blended attacks include deep packet inspection (DPI) firewalls, intrusion prevention and "behavior blocking" — tools that alert on unusual software activity — and, of course, ensuring that your users know what not to click on.

3 End Runs

While many attacks start by "pounding on the front door" — hitting the gateway that connects your local area network (LAN) to the Internet — many will go around, possibly never even touching the network en route to a computer.

Gateway-level security won't protect computers from threats on CDs or USB (Universal Serial Bus) flash drives. Nor will it protect an employee computer or handheld that's being used outside the office, such as in a wireless hotspot, where eavesdroppers or rogue access points (APs) may intercept traffic if the machine being used doesn't have sufficient client-level security. These attacks are called end runs.

According to "Network Security and Intrusion Prevention," a January 2005 survey of 250 North American security professionals conducted by Enterprise Strategy Group (ESG) Research, Milford, Maine, infected employee notebooks make up 39 percent of worm attacks that get into a company LAN. The second most common source was through the firewall, followed by nonemployee notebooks and virtual private networks (VPNs) connected to home systems. "Three of the top four sources of this threat went around the firewall," says Jon Oltsik, senior analyst at ESG Research. "This is why multilayered 'defense in depth' threat management is necessary."

Some threats can go right through older gateway-level security, which may not recognize threats that are spread across multiple packets or don't match their database. DPI and URL/content filtering and blocking play an important role in this type of threat prevention.

4 Rogue Access Points

Rogue access points — APs that don't belong to IT or aren't configured by IT to reflect company security policies — represent a major network security threat. They can allow unauthorized parties to eavesdrop on network traffic and attempt to inject threats. Once a rogue AP has been connected to the network — which can be as simple as plugging a Wi-Fi adapter into a USB port, connecting an AP to an untended Ethernet port or using a Wi-Fi-equipped notebook or handheld computer — an unauthorized user may be able to access your network from outside the building or even further away.

Features for detecting rogue APs and blocking their access are available in many new wireless switches, as well as in gateway-level Unified Threat Management (UTM) security appliances from such vendors as Cisco, Juniper, SonicWALL and WatchGuard. UTM appliances take the place of separate single-purpose security devices, reducing cost and management. Capabilities include firewall, VPN, intrusion prevention, antivirus/antispyware and content/URL filtering. Increasingly, UTM appliances have a range of security engines built in. IT can then choose which modules to pay for and activate.

5 Web and Browser Exploits

Web exploits attempt to breach security through Web servers, such as Microsoft IIS Apache, Sun's Java Web server and IBM WebSphere. Successful attackers may gain complete control of systems, allowing unauthorized access to directory listings and the ability to create new accounts and read, change or delete data. According to the Common Vulnerabilities and Exposures list compiled by the MITRE Corporation, a not-for-profit technology research and development organization, roughly a quarter of the security flaws from 1999 through 2005 were Web exploits.

Browser exploits, similarly, seek to take advantage of security vulnerabilities in users' Web browsers due to unpatched versions or unsecure configuration. Malicious JavaScript, ActiveX or Java applets can, for example, crash user computers, download "backdoor" or other malicious code, giving intruders full access to the computer. Successful attacks can steal user logins and other sensitive data and compromise user computers.

Solutions include URL/content filtering at the gateway, switch and client levels, running vulnerability scanner software to check Web servers and client systems for potential vulnerabilities, applying security patches, and configuring Web servers and browsers securely.

6 Worms and Viruses

Viruses, which infect existing computer programs, and worms, which are executable programs, are some of the oldest and most well-known types of computer threats. Viruses tend to be in document, spreadsheet and other files and spread via e-mail, while worms typically spread themselves directly over networks. Once a worm or virus has infected a computer, it may begin wreaking havoc in addition to attempting to replicate itself to other systems.

To protect against worms and viruses, run antivirus software both at your gateway and on your computers. Also, consider also using secure switches inside your LAN. Most of all, be sure to keep your antivirus definitions and software up to date.

7 Information Theft

Your company's information includes user names and passwords, which can be misused to gain access to databases, applications and systems. Lost, changed or compromised names or passwords can, in the wrong hands, put your company at risk from regulatory fines, loss of business and other costs.

Preventing information theft requires securing your network to keep unauthorized users away and also block unauthorized attempts to extract sensitive information. Solutions include gateway-level firewalls, intrusion prevention, antivirus, antispyware, spam blocking and URL/content filtering, as well as the use of VPN connections for mobile and other remote users, Network Access Control (NAC) and endpoint security to ensure that client devices are secured. (Don't forget physical security of your facilities and proper disposal of paper, computer media and hard drives.)

8 Phishing

Phishing simply attempts to fool end users into believing that bogus e-mail, phone calls or Web sites — often related to online banking and payment services — are legitimate, with the intent of getting them to provide private information or download hostile applets to infect the user's computer. According to SonicWALL, over six billion phishing e-mails are sent worldwide each month.

"Phishing is one of the harder threats to protect against, because it's more about [exploiting] human behavior," says Sanjay Beri, director of product management, security products group, Juniper Networks. "Web filtering, which blocks requests to sites identified as phishing sites, helps a lot. If an employee tries to go there, they'll get a message indicating it's a phishing or otherwise restricted site."

To prevent phishing, look for gateway-level security that examines incoming e-mail and Web code. Consider adding outbound blocking — blocking e-mail and URLs from browsers to known or suspected phishing addresses.

9 Keystroke Logging

Keystroke logging, or keylogging, refers to programs that can record a user's keyboard (and possibly mouse) input to get user names, passwords, e-mail, instant messages and other employee activities. Keylogger programs typically capture this information to a file, and then surreptitiously forward these files for identify theft or other misuses.

The most common method of keylogging is using spyware or other unauthorized programs on a user's computer. Other approaches include electronic eavesdropping — hardware devices snuck into keyboards or a computer's USB or PS/2 ports. Along with vigilance, DPI and URL/content filtering are key defenses.

10 Instant Messaging Vulnerabilities

Like e-mail, instant messaging is a common vector by which viruses and spyware spread, typically through sent files that users open. "When employees use IM and peer-to-peer applications, they can easily download spyware without being aware of it," says Jon Kuhn, director of product management, SonicWALL Inc. "And often, once opened, an IM virus will resend itself to everyone on the user's contact list, as well as installing spyware."

To prevent IM-borne threats, use network, switch and client antivirus/antispyware tools, keep computer operating systems and IM applications up to date — and teach employees not to click on unrequested files. ◊