Chapter 13

HOLDING YOUR DEFENSIVE LINE

INTRODUCTION

The Internet is a two-edged sword for most enterprises. On the positive side, the web provides easy access to information, fosters collaboration among partners and vendors, and can increase employee productivity. The web augments established distribution channels for many enterprises and is the sole distribution channel for others. Most enterprises could not exist today without a web presence and with a substantial portion of their workforce provisioned to use Internet resources as part of their daily work [1].

With so many employees accessing the web, IT leaders are becoming increasingly familiar with the problems and risks of unfettered Internet access that add up to a significant down side. Employees may spend too much time surfing the web for personal use, reducing productivity.

> **Note:** According to industry analysts, the average computer-enabled employee spends 12.6 hours per week accessing the Internet with 3.6 to 6 hours spent on non-work activity.

Worse, they may visit inappropriate sites that may present legal liabilities. They may link to sites that are the source of malware, inadvertently downloading spyware and keyloggers. Employees who download music or videos from Peer-to-Peer (P2P) file-sharing sites risk involving the enterprise in lawsuits filed by copyright owners. Even legal purchases of music and videos from authorized sites may consume a disproportionate amount of the enterprise's external bandwidth, driving up costs [1].

Employees may also discuss enterprise-confidential business over unsecure Instant Messaging (IM) services or open infected IM attachments that unleash malware behind the perimeter firewall [2]. The situation has become critical. Enterprises need the web in order to conduct their business, yet they are losing employee productivity and are threatened by new web-borne attacks that may cause significant damage. The drain on employee time and network resources is well known: In one industry analyst survey, a quarter of enterprises reported terminating workers for Internet misuse. A solution is needed that will allow managers and their employees to use Internet resources with appropriate measures

of flexibility and responsibility. The enterprise needs to hold its defensive line (hiding passwords; implementing packet filters; adopting strong authentication with Kerberos and other tools; and, authenticating users with public key encryption) against employees who would allow masqueraders to infiltrate its systems [1].

TROUBLE ARRIVES ON PORTS 80 AND 443

To facilitate web connections and content delivery, Port 80 is the designated port for web traffic using HTTP. Similarly, Port 443 is the conduit for HTTPS traffic which is HTTP encrypted using SSL, the Secure Sockets Layer built into all standard web browsers. The result is that Ports 80 and 443 are always open on most enterprise firewalls. There is generally no attempt by perimeter firewalls to inspect, analyze, or otherwise impede the flow of traffic through these ports [1].

Knowing that these ports are open, vendors have designed their products to use them to communicate with locations behind the firewall. For example, most Instant Messaging protocols default to Port 80 if their designated port is blocked. The same is true for many P2P file-sharing protocols. These web ports have become four-lane off-ramps from the information superhighway [1].

INCREASINGLY SOPHISTICATED CRIMINALS/MASQUERADERS TARGET THE INTERNET

Criminals/masqueraders have also recognized that Ports 80 and 443 are open doors and have devised clever ways to exploit this vulnerability. While early attacks added malware extensions to P2P protocols or Instant Messages, more recent attacks have been perpetrated using:

- False web sites that take advantage of mis-keyed URLs
- Phishing scams that send phony e-mails directing people to counterfeit sites where they must enter financial information to update their accounts
- Pharming frauds in which an enterprise's DNS servers are corrupted so that even users who enter valid URLs are unknowingly redirected to fake sites
- Drive-by downloads in which merely visiting a URL can automatically download unwanted applications including keyloggers and Trojan horses
- Unintended linkages to sites with hard-to-eradicate pop-up ads and spyware [1]

> **Note:** Spyware is a broad category of malicious software intended to intercept or take partial control of a computer's operation without the user's informed consent. While the term taken literally suggests software that surreptitiously monitors the user as a spy would, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party (see: http://en.wikipedia.org/wiki/Spyware).

The purpose of attacks has changed as their level of sophistication has increased. Early malware was aimed at creating problems or causing disruption – exploits that became a