The Web: Mobsters extinguish firewalls

May 3 2006

Firewall? Forgetaboutit. Cyber-criminals, including the mafia, are now so savvy they can penetrate past these supposedly sturdy security measures and hack your computer network, whether you work at a university, Fortune 500 company or smaller firm, experts tell UPI's The Web.

"The firewall and the network perimeter are dead," Ted Demopoulos, author of the best-selling book, "Blogging for Business" (Kaplan, 2006), and IT expert based in Durham, N.H., tells The Web. "Firewalls offer less protection than before."

The mobsters -- and their teenage hacker employees -- are accessing servers in a number of ways. They are tunneling into computers, directly, through the so-called Port 80 on every PC, posing as legitimate Web traffic. They are also sneaking into networks through "extranets," or private connections to the corporate network, accessible with a password and user name, through an interface available over the Internet. They are also exploiting wireless access points -- WAPs -- set up to enable employees to work wirelessly throughout an office complex, or collaborate remotely, away from the office.

"Cyber-crime is big business now," said Demopoulos. "Some claim it surpasses the illegal drug trade. It's not teenage hackers anymore. For-profit criminals, with substantial resources, are behind the Internet crime wave."

Criminals are even penetrating the most run-of-the-mill commercial

operations over the Internet -- like college bookstores -- to make illicit gains. Experts at AmbrionTrustWave, a Chicago-based information security company that serves 25,000 clients around the world, indicate that an "unauthorized individual" recently hacked into the network at a university bookstore, over the Internet, and stole "thousands of students' -- and their parents' -- credit card numbers." The hackers figured out that the point of sale system in the bookstore ran on a dated version of Microsoft Windows and was connected to the Internet.

In fact, experts say, universities are increasingly becoming targets of cyber-criminals because of lax security implementation. Universities, unlike companies, generally function in a decentralized fashion regarding their IT infrastructure. Every department may have a different IT infrastructure, budget, operations, decision-making structure and compliance requirements. What is more, universities operate on the idea of "openness" and exchange of ideas, something criminals are now starting to exploit.

One tool that IT departments are using to prevent security breaches, now that firewalls and spam filters can be penetrated, is so-called SSL certificates. SSL stands for secure socket layer in computerese. "VeriSign has seen the rising online trend of phishers and cyber-criminals becoming increasingly sophisticated in the types of attacks they are launching to navigate spam filters and steal consumer information," a spokesman for VeriSign, a leading IT software firm, told The Web.

The SSL software grants access to Internet resources on a step-by-step basis, after conducting several tests for authentication. The technology is also being used on Internet sites to demonstrate to consumers that they are not visiting a make-believe site, established by Tony Soprano's second cousin from Philly. "As phishing has increased dramatically, visitors to e-commerce sites, online banks, and the like have begun to

look for the presence of an SSL certificate as a sign they are attached to a real site," said the VeriSign spokesman.

Another oft-discussed way to keep hackers at bay is biometric security devices. These devices, which use fingerprint authentication and other biometric data are quite expensive to establish, however, and are complicated to implement. A spokesman for Silex Technology America, which makes Bio-NetGuard, tells The Web the system integrates a Fujitsu MBF200 sensor, which can match fingerprints in 400 milliseconds.

But unless businesses and universities and others are willing to install the readers and sensors at every PC location and every WiFi hotspot, the technology may prove impotent in the fight against cyber-crime.

"Traditional organized crime is slowly moving, like any big business, onto the Internet, and is a new breed of entrepreneurial criminals," said Demopoulos.

As the mobsters, or at least their cinematic counterparts might say, it's nothing personal. Only business.