REDHERRING

WEB APPLICATIONS

The weakest link.

By Jennifer Lewis

NOT SO LONG AGO, companies did whatever it took to get onto the Web. That often meant unintentionally opening holes in their network security to provide access privileges to suppliers, customers, and partners. They've since installed newer security products to mitigate these vulnerabilities, but they haven't gone far enough: an area left relatively unprotected is the Web application, a serious weakness in their systems.

Hackers are well aware of the situation. They have begun exploiting these weaknesses, using sophisticated tools to deface Web sites that host applications or to plant malicious codes that can be activated at a later time.

Several startups, like Sanctum, Kavado, and Ubizen, have recently developed software that protects against these kinds of attacks. The software first tests a Web site from within the network to reveal any weaknesses that could be exploited by intruders, then automatically installs security patches for the holes it has detected. It resides between the Internet and the Web server and functions like a proxy, filtering incoming traffic from the Web, blocking HTML pages and other unauthorized data, and only allowing legitimate requests to reach the Web server.

Application-level security costs approximately $15,000 a server, depending on the number of servers being protected. This may seem expensive, but most companies will consider this as insurance. After all, when the Internet worm Code Red hit the Web in July it caught companies completely by surprise, inflicting an estimated $1.2 billion in damage to networks.

Before these Web-application security products existed, system integrators had to patch each server manually. Because there were so many holes to patch and so few skilled security professionals to do the patching, companies faced a human-error problem as well. "Hacking is increasing at the application level because there has been very little invested there," says Peggy Weigle, CEO of Sanctum. "The hackers are simply going where the low-hanging fruit is."

Companies like Sanctum hope to get a chunk of the healthy Internet-security market, which the research firm IDC expects to nearly triple to $14.2 billion by 2005, from $5.1 billion in 2000.

Based in Santa Clara, California, Sanctum was one of the first security companies to focus exclusively on application-level security. Among its 300 customers is NetVision, Israel's largest ISP. NetVision has been using Sanctum's AppShield to protect its customers, which include the Knesset (Israel's parliament) and Israel's Ministry of Foreign Affairs.

But Sanctum isn't the only player in the market. Ubizen, a spin-off from Katholieke Universiteit Leuven (Belgium's largest university) and one of the most diversified of these security companies, has more than 500 employees spread across offices in nine countries. It has recently developed an application-level firewall called the DMZ/Shield, which protects files and other network resources.

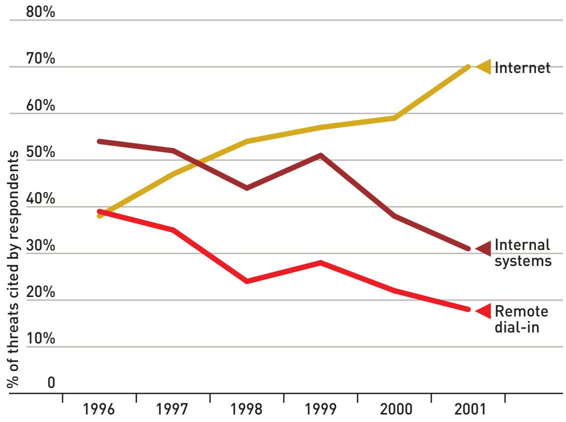
Founded in February, New York–based Kavado, is the newest player in the Web application–security space. In July, it raised a $3.7 million second round of funding, led by 3i Technology Partners. It claims that its software is more plug-and-play, more dynamic, and much faster to get up and running than competing products. Like other security companies, Kavado won't release customer names.

A company is only as strong as its weakest link. In spite of all the network security in companies today—firewalls, virtual private networks, public-key infrastructure, antivirus software, intrusion-detection systems—there's still a need to be extra vigilant and protect against intrusions through Web-based applications. However, according to Taher Elgamal, who helped develop the secure sockets layer encryption protocol for Web transactions and is currently CEO of the security-service provider Securify, this additional security only protects against application-level problems, which is only one of the ways an attacker can get in. Most companies, however, are still lax about application security problems, so it will probably take at least a year—or a few costly attacks—before companies wake up to the threats and purchase defenses against them. ■

Write to letters@redherring.com.

ATTACK LOG

Increasingly, Internet connections are cited as a point of attack, while threats to internal networks have fallen off.



REPRINTED FROM ISSUE NO. 109, JANUARY 2002 • PHONE: 415/865-2277; FAX: 415/865-2280; WWW.REDHERRING.COM