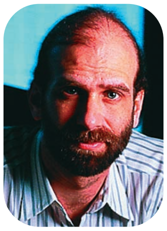
The Speed of Security

The Slammer worm was the fastest computer worm in history. As it began spreading throughout the Internet, it doubled in size every 8.5 seconds. It infected more than 90 percent of vulnerable hosts within 10 minutes." (See "Inside the Slammer Worm," p. 33 of this issue.)



BRUCE SCHNEIER
Counterpane Internet Security

For the six months prior to the Sapphire (or SQL Slammer) worm's release, the particular vulnerability that Slammer exploited was one of literally hundreds already known. Microsoft provided a patch, but many ignored it (so many patches, so little time). However, on 25 January 2003 at 05:30 UTC, installing that one patch suddenly became the most important thing system administrators could do to improve their security. A day later, a system administrator could install hundreds of other patches, but no one knows which patch will become the next vitally important one, or when.

Traditional computer security has been static: install a firewall, configure a public key infrastructure, add access control measures, and you're done. That might have been enough 10 years ago, when attacks traveled slowly and attack tools were primitive. However, on today's Internet, security is a moving target, so it must be dynamic.

Attackers are clever and devious and their attacks are subtle and difficult to detect. New vulnerabilities constantly appear, and unimportant vulnerabilities become important overnight. Worms and viruses infect the globe in minutes. Information about vulnerabilities spreads through the attacker community overnight, and new attack tools become popular within weeks. To maintain security, defenders must be faster. Last month's security sometimes feels only slightly better than no security at all.

All of this points to security monitoring. Firewalls, intrusion detection systems (IDSs), and other security products are essentially security sensors, constantly providing information about what's happening on a network. To make security work, you must monitor those sensors, in real time, 24/7. Products alone can't do this; monitoring requires people—trained security experts. These experts must have the knowledge and expertise to quickly separate false alarms from real attacks and know how to respond to them. They must be able to adapt to new situations and vulnerabilities in minutes. New threats can come from anywhere on the globe. If experts monitor the health of the entire Internet—not just one single network—they're going to do a much better job.

This isn't something an organization can do itself. Security monitoring must be outsourced. Just as we outsource our public safety to police organizations and our public health to doctors and hospitals, the economies of scale associated with Internet security are such that there's really no alternative. It's simply too expensive for any but the largest companies to build the necessary monitoring infrastructure and staff it with the necessary experts. And even if they did, they couldn't do nearly as good a job as a large-scale outsourced organization that monitors several networks across the globe.

Gartner, the analyst firm, recently released a report decrying problems with IDS (www.gartner.com/5_about/press_releases/pr11june2003c.jsp). One of the major problems it cited (and a reason for not installing an IDS) was this: "An increased burden on the IS organization by requiring full-time monitoring (24 hours a day, seven days a week, 365 days a year)." Yes, one of the problems with security today is that it requires full-time monitoring. But the solution isn't not to install security products—that doesn't change the threat—but to figure out how to do the required monitoring cheaply and effectively.

Security is a process, not a product. Security based on monitoring is security that recognizes human intelligence is vital for a strong defense and that automatic software programs just don't cut it. Security recognizes attacks can happen any time, day or night, and is ready for it. Security works in an era of worms that can spread across the Internet in 10 minutes. □

***Bruce Schneier** is one of the world's foremost security experts and Counterpane Internet Security's Chief Technology Officer. His new book,* Beyond Fear: Thinking Sensibly about Security in an Uncertain World, *will be published by Copernicus Books in September. Contact him at schneier@counterpane.com.*