Does Your Network Security Address Every Layer

By Elizabeth M. Ferrarini

WE'VE ALL SUFFERED FROM SPAM ATTACKS EITHER AT WORK OR AT HOME At one time, you could put productivity concerns aside while you cleaned your your inbox. Today, however, spam brings viruses and other pesky payloads along for the ride. Remember, the MyDoom and SoBig threats? Together, these worms and their variants—both of which used spam technology to spread viruses—caused billions of dollars' worth of damage around the world. Spyware also threatens businesses on more than one level—capturing confidential data like passwords and customer information while degrading system performance at the same time.

It turns that help is readily available. On the other hand, you'll find so many providers and options to evaluate, even the largest businesses with the biggest IT staffs have difficulty keeping up with all of them. Identifying and plugging the holes is half the battle. Often, the resources needed to keep security up-to-date far exceed the initial purchase price of the security solution.

Regardless of the threats, many organizations, especially small to midsize ones, don't have the time or the resources to spend on adequate security.

Regardless of the threats, many organizations, especially small to midsize ones, don't have the time or the resources to spend on adequate security. Although they want to keep all hands focused on the core business, they often get bogged down by the sheer number of threats, their complexity, and their increasing damage.

By examining security in holistic layers, organizations can begin to think about security more proactively. This technique makes it easier to understand how to defend your business—its data, applications, and networks—and to keep that protection updated. The six security layers include the following:

Physical Security Layer – This layer protects IT gear from being stolen with tools like chassis and cable locks. You might want to move your servers out of publicly accessible areas, such as closets. You should also consider locks, cables, and brackets to protect not only your mobile and desktop computers, but also valuable peripherals.

The Data Security Layer—It restricts access to confidential information. Start by requiring strong passwords which use longer, non-obvious combinations, such as alphanumerics and symbols. Depending on your industry or experience, you might want to use smart cards, biometric security, or other rigorous authentication options. An investment in centralized credential management and self-service password resets can pay off immediately. Also look for desktops and mobile PCs that have a chip which can encrypt sensitive credential information, such as IDs, passwords, encryption keys, and digital certificates.

The Application Security Layer—It protects against application-destined viruses, worms, and threats that can result in corruption or inaccessibility. To detect, remove, and prevent future threats like these, install anti-virus solutions (Norton Anti-Virus), run the scan regularly, and make sure you update the program to add protection from new threats. Application-level firewalls can protect applications, such as Microsoft Outlook or Web-based systems.

The Network Security Layer—It uses tools, such as application-level firewalls, to block unauthorized network access. Because most viruses are contracted via e-mail, an application-level firewall can provide critical protection for those organizations with only network-level firewall protection. Hardware firewalls and virtual private networks provide excellent strategies for network security and should be part of a company's arsenal.

The Security Management Layer—It assesses the vulnerability of the business environment and manages patches and updates. Gathering, testing, disseminating, and installing the huge number of daily new patches for all servers and all PCs can consume a lot of an IT department's time and energy. You might want to adopt a single-console solution that enables you to assess and to identify threats and vulnerabilities, automatically deploy patches, and report on the status of your systems.

The Security Policy Layer—It provides the underlying guidelines and training requirements for carrying out security. Policies can include things such as a desktop lockdown which limits a user's ability to change desktop configurations, install rogue applications, or add/remote peripherals. This technique can prevent illegal file-sharing or unauthorized copying of company data. IT personnel need to be trained to understand and to identify security threats, such as phishing.

By investing in tools and techniques to reinforce each of the six security layers, you can prevent catastrophic damage that could cripple business. If you're, however, not sure of your IT infrastructure, you might want to work with a security consultant who can identify vulnerabilities, review your policies, test your security, share best practices, and make cost-effective recommendations.

NaSPA member Elizabeth M. Ferrarini is an IT consultant from Boston, Massachusetts.