BIG SECURITY IN SMALL PACKAGES

Gateway security appliances offer cost-efficient protection with minimal fuss.

Today, every business is connected to the Internet. And that means every business is under attack.

First it was viruses, then worms, Trojan horses and spam. An expanding array of exploits — SQL injections, cross-site scripting, phishing and more — soon followed.

Today, drive-by attacks can infect a network just by a single employee's visit to a hacked site. And just about any website can be hacked.

Security appliances offer effective, easy-to-manage protection for small-business networks. They work by bundling a range of security functions into a single device: firewall, antimalware, intrusion detection, spam filtering and more.

For businesses with limited resources to spend on network administration and limited labor-hours to spare, unified threat management (UTM) appliances offer enterprise-level security. And they do it without the need for enterprise-level staffing.

Whether a business is a five-person shop or a 50,000-person enterprise, inadequate security can spell trouble. Fortunately, firms are discovering the flexible, convenient and state-of-the-art security found in security appliances.

Under Attack

In the past, it was easier than today to trust in the notion that a small business often presented too measly of a target for attackers to trouble themselves with. A firewall and a good antivirus suite seemed like more than enough protection to handle whatever threats the Internet might present.

Those days are long gone. The reality now is that every company with an Internet connection is a target. And virtually every company has an Internet connection.

"It's not like bad guys are out there targeting this person or that business," says Tracy Hillstrom, senior product manager at WatchGuard Technologies. "Hackers are just looking for resources, and they have automated tools to exploit them. Once a hacker has deployed these tools, it's only a matter of time before they come across a way to make money — often at a small business's expense."

Those resources could be an e-mail server hijacked to send spam, a desktop computer used to launch a denial-of-service (DoS) attack against a website or a database full of customer credit card numbers open to exposure. "Hackers are being less picky about what they're going after," Hillstrom says. "They go after whatever is open."

In the past, viruses and worms generally required computer users to make some sort of mistake to infect a system, whether visiting the kind of site that most businesses generally consider off-limits or opening an attachment from an unknown party. Today's attacks can happen quickly, silently and often without any action on the part of the user.

Web pages on more than

560,000 WEBSITES

were infected with malware in the fourth-quarter of 2009.

Source: Dasient

"The main vector through which attacks come today is the web," points out Jason Leung, senior product line manager for security solutions at NETGEAR. "All the websites that we frequent today include components of sophisticated technologies — Flash, SQL, JavaScript — that allow them to produce a rich media experience for their users.

That means each website has much more code," he adds. "And more code means more vulnerabilities and opportunities for bad guys to create malware to attack your system."

For example, hackers exploit common technologies to install malicious code onto a company's computers without employees even noticing. This is the same know-how that lets YouTube videos start playing as soon as the page loads, pop-up ads to open automatically, and different pages to be displayed depending on whether a user is logged in or not.

And it's not just porn and warez sites that pose a risk. Last year, mainstream sites ranging from Fox Sports to the gadget blog and second most popular blog in the world, Gizmodo.com were infected.

Closing the Front Door

Despite the severity of the threats facing today's small businesses, the situation is not entirely grim. As hackers' methods have evolved, so too have security experts' understanding of how to protect against threats.

Security today is based on a fundamentally simple concept: layers of nested protection, one inside the other. Attackers who

manage to pierce one layer then find themselves confronted with another layer and another after that will move on to less guarded data.

Defense in depth works "like pages in a book," Hillstrom says. "You have to go through all the pages, one at a time, to get to the end."

This is why you can no longer depend on just firewall and antivirus applications running on individual desktop or notebook systems. Although these play important roles in an overall security strategy, they act as only a single layer — if hackers manage to get through at the endpoint, it's essential that the network make sure they get no further and so are unable to spread malware throughout the company's networks and systems.

Before malware can reach a computer on the network, however, it has to go through the gateway, where the network connects to the Internet. By placing layers of security at the gateway, a company can filter out most attacks before they ever reach a desktop or server.

Gateway security comprises three functions, says Brad Sakai, manager of the small business technology group at Cisco Systems. "The first is the firewall, which blocks anyone outside from visiting your network and makes sure every exchange is initiated from inside the network." A solid firewall is crucial, but it is only the first step.

"The next level is intrusion prevention, which goes beyond scanning who the data is from and looks at the actual content to see if it matches a known pattern," Sakai explains. "Then beyond that is application filtering, which prevents access to sites that are known to be dangerous."

Of course, this last tool's policies must be set to apply to traditionally questionable sites. And it must also be increasingly set to legitimate sites that have become infected.

The Cisco ProtectLink Gateway service, an option available with its SA 500 Series Security Appliances for small-business, and WatchGuard's Reputation Enabled Defense Solution, which is available on XTM 2 Series appliances, maintain a list of known infected sites against which all traffic through the gateway can be compared. This approach effectively updates a corporate blacklist on the fly as newly infected sites are discovered.

Small Business-Sized Security

"The needs of small business are not particularly different from the needs of enterprise," says Alex Gray, senior vice president and product manager for Juniper Networks. "The only difference is one of scale."

Large companies rely on single-purpose dedicated devices to process their vast network traffic. This, in turn, demands that they maintain a large staff of IT professionals to tend to those security systems.

"Smaller businesses can't afford a conga line of devices," points out Gray, referring to a daisy chain of single-function tools that can often be found in enterprise security systems. Instead, security appliances such as the Juniper SRX Series of security gateways — aimed at small businesses and branch offices — integrate firewall protection with intrusion prevention, antivirus, antispam and web filtering.

"Our approach is to bring down our full enterprise suite to the small-business scale," he adds. "Here user experience and cost of ownership is adapted to the SMB [small- and medium-sized business] customer."

Because UTM appliances combine all the layers of an effective security system in a single device, NETGEAR's Leung calls his company's UTM gateway line "a Swiss Army knife — and Swiss Army knives are pretty good tools." NETGEAR's Stream Scanning Technology collapses the process of receiving, scanning and forwarding data into a near-simultaneous event, speeding up legitimate network traffic by reducing latency as the UTM scans for viruses, malware and other signs of trouble in the data stream.

The benefit of such an approach is that all the tools needed reside in a single place and function similarly. Because all the security tools use the same interface to configure and monitor a network, the IT team will spend less employee time managing security, whether it's handled in house by a member of the staff or by a third party, who can even manage security remotely using the device's web interface.

The Cost Factor

Installing a UTM appliance obviously requires a smaller initial expense than installing multiple specialized, single-purpose devices. Costs will remain lower over the long run as well because fewer IT hours will be spent on managing security — or recovery if something goes wrong.

In addition to quantifiable savings, solid security architecture offers a range of less easily measured benefits that add up to a significant return on investment. The value of strong gateway security lies largely in what doesn't happen and how it affects worker productivity.

"Small businesses are very sensitive to how people spend their time," notes Chris Christiansen, program vice president for IDC's Security Products and Services group. For instance, blocking spam at the gateway, before it reaches workers' desktops, frees up

Security Spending to Increase Despite Economy

Few thoughts keep IT chiefs awake at night more than data security. A single breach can wreak havoc on operations, frighten customers and torpedo profits. Unfortunately, protecting the tangle of systems that can span offices and continents is a daunting proposition.

The current sluggish economic environment only increases the difficulty of the task. The global recession has heaped growing pressure on businesses to keep budgets in check and maximize the return on investment for all IT endeavors.

In spite of a slow economy, both large and small enterprises report that they will spend a higher percentage of their IT budgets on security in 2010.

Salient Security

According to Forrester Research, approximately 40 percent of businesses will significantly boost spending on new IT security technologies this year.

According to two studies released by the company, "The State of Enterprise IT Security and Emerging Trends: 2009 to 2010" and "The State of SMB IT Security and Emerging Trends: 2009 to 2010," nearly half of enterprises surveyed expect to increase IT security spending on new technologies by 5 percent or more this year. Furthermore, 37 percent of small and midsize businesses expect to do the same.

Interestingly, IT security pros are not as worried about security demands driven by cloud computing and virtualization as they are by the proliferation of consumer devices in the workplace, such as smartphones and other portable systems that act as mobile endpoints.

Justifying Spending

With budgets tight, there are ways to invest wisely in network security. First, any area that can impact revenue will take priority with management. Also, be sure to promote projects that offer maximum ROI.

Industry experts also suggest approaching the topic from management's point of view. That means look at ways to optimize the network so that a single management infrastructure can support multiple solutions. For small businesses, this is especially important, so that limited IT staffs do not waste time learning and managing several independent and unrelated systems.

employee time to work on tasks more valuable and strategic than deleting unwelcome e-mail.

Likewise, preventing employees from visiting websites that may pose a threat has the added benefit of keeping them from wasting time on nonwork pursuits. This is an even bigger bonus if it means they are unable to engage in illegal activities such as sharing copyrighted files, which could create a liability issue for the employer.

Of course, the biggest threat to worker productivity is loss of data or network services caused by malware and other network intrusions. "It's pretty hard to determine the value of a lost customer list or the value of lost trust if customer information is sold to a criminal organization," Christiansen says.

"On a simpler level, it's easy to see the level of business disruption from a malware infection that lasts several days," he adds. "Or consider an attack that disrupts or disables all the IT systems, key software or Internet access."

Small businesses, especially, cannot afford the cost of inadequate security. There is simply too much at stake with every given customer, client or transaction, and the competition from bigger companies too severe, warns Christiansen. "Every disruption of business is a disruption of a service to a customer," he says. "And a customer can always go somewhere else."

Unified threat management offers small businesses the opportunity to protect themselves against such disruptions. They can wrap up the layers of security a gateway needs in a single affordable and easy-to-manage package.

"What small businesses need to realize is that they are being attacked the same way larger businesses are," WatchGuard's Hillstrom says. "Enterprises use a complex defense-in-depth strategy with many layers. UTM devices mirror that approach at a level that small businesses can take on." ■