

Small business a big target for cyber attacks

by Stefanie Hoffman

Once upon a time, most small-to-midsize businesses enjoyed a relatively secure status, free from malicious cyber threats. Not so anymore, experts say.

"It used to be that SMBs were not a target just because of how small they were," said Andy Klein, senior product marketing manager, e-mail security division for SonicWall Inc., Sunnyvale, Calif. "So they could put up a Web server and no one would ever see it. But that's changed. Two, three, four years ago, you could say that you're willing to take the risk and put up a firewall and call it a day. I don't think you could do that anymore. If I have a tool that I can use to thwart a lot of reputations systems, what better place than to attack small organizations that don't have infrastructure in place?"

If anything, SMBs are a target now more than ever before. Malicious security threats—particularly those executed via the Web—are abundant as an unprecedented number of botnets, Trojan horses and self-replicating worms, created and executed by organized criminal networks, are unleashed on networks to steal personal and financial information.

While SMBs might have already secured some vectors, such as e-mail and the network perimeter, others have been flung wide open. Security experts say that 2007 was a record year for malware attacks launched through the Web, with an exponentially growing number of attacks that used legitimate sites as the vehicle to spread malicious code and infect users.

"We're not dealing with the junk boot virus on a bunch of floppies," said Luke Walling, president of Walling Data Systems Inc., Claremont, N.C. "It's a lot more dangerous and a lot more difficult to control. Their goal is to sit in the background and log data so it's not obvious that you're infected."

Yet, for SMBs, re-educating employees to change their Web behavior represents just one more thing to worry about.

"There's a different problem with Web exploits," said Rick Carlson, managing director for North America of AVG Technologies, Chatsworth, Calif. "People can grasp what spyware is. They can't really grasp what Web exploits are. The payload could be anything. The name of the game is to make that machine operate as normally as possible."

A lagging economy has caused many companies to rein in their IT budgets, opening SMBs up to attacks simply because they lack the money and staffing for proper security infrastructure, experts say.

Along with a lack of resources inevitably comes a lack of awareness about security issues. As a result, SMBs often have a huge gap in their security policies regarding behavior and best practices. Meanwhile, even if an SMB is fortunate enough to have an IT person on staff, chances are he or she is overworked and challenged to convince administrators to allocate more funds toward security. "There's not a big sense of urgency about it," said Stephen Kolbe, president of AnalySys Enterprises Inc., a Baltimore-based IT solution provider.

"We're not dealing with IT departments. We're dealing with business owners. They're relying on us as consultants to tell them what they need."

Partners say that the first step is to comprehensively evaluate the nature of the SMB's security environment. That includes both internal as well as external threats.

SMBs now require a multilayered approach to adequately secure their networks and data. This initially includes a perimeter solution and antivirus/antispysware coupled with an application layer that protects information. The client can subsequently build out from there with things like an affordable SSL VPN solution. Partners also maintain that because each SMB's security environment is unique, multilayered solutions should probably incorporate a variety of cost-effective, alternative technologies specifically tailored to meet the specific needs of their security environment. Those products can often—and should—be implemented in phases to make costs more palatable.

"You really need that multilevel approach for security today," Walling said. "We look for smaller vendors to do what everyone else is doing but doing it a little bit different and, in our opinion, a little bit better."