PRONET smallBusiness RESOURCE CENTER

Computer Security Solutions

Published August 01, 2007

Five real tools you need in order to protect your business from virtual threats.

By: MATT ALDERTON

Viruses. Spyware. Identity theft. To the average ear, it all sounds like pieces of the plot to a bad made-for-TV thriller. In fact, though, these aren't soap opera elements. They're security threats, and they could cripple your business.

"The vast majority of companies in the United States have less than 20 employees, and these types of companies have data that is just as important to protect as companies with 10,000 employees, such as social security numbers, credit card numbers, etc.," says Pittsburgh-based IT consultant Bob Stein, a Microsoft Most Valuable Professional and co-founder of ActiveWin.com. "In many cases, security to small businesses should be considered more a concern than to large companies because they are more vulnerable."

According to Stein, the biggest mistake that small businesses make when it comes to security is complacency. Small enterprises assume they're not important to hackers and saboteurs—and they couldn't be more wrong.

"They have a 'It's not going to happen to me' attitude when it comes to security," he says. "If you have that attitude, sure enough something will happen."

Rather than plead ignorance, small business owners should assume something *will* happen, Stein says, and proceed accordingly. That is, they should be prepared in order to protect themselves, their business and their customers, as security threats can hinder your connectivity, damage your integrity and altogether stall your productivity.

Preparation doesn't have to cost a lot, either, according to IT consultant Richard Lee, founder and president of New York-based Pillar Consulting Inc. "I am always a big proponent of 'Do it yourself,'" he says. Small business owners—even the least tech savvy among them—can secure their networks and their information with less than $100 worth of easy-to-install software and peripherals.

So what do you really need to secure your small business mainframes? Start with these five essentials:

1. Firewall

Perhaps the most essential piece of computer security is a firewall, according to Jim Gutman, a Phoenix-based franchisee of 1 800 905 GEEK, a Norfolk, Va.-based chain of computer service technicians. A firewall, he says, lets you and your employees access the Internet via your network, but blocks Internet users outside that network from accessing your computers.

"Whether you're in an office or at home, the first thing you should be doing is look at putting up a router," Gutman says.

Firewalls can be either hardware- or software-based, and a router—like one from Linksys—functions as a hardware-level firewall, he adds; it lets you go outside of your network and prevents others from coming inside it. Hardware firewalls are automatic, while software firewalls often require manual controls.

2. Anti-Virus Software

Next to a firewall, every business—large and small—needs anti-virus software, according to Gutman, as an unchecked virus can wreak havoc on your system.

"What people don't realize is that their entire neighborhood or their entire office complex is basically on the same local network," he says. If a virus gets to one of your neighbors, therefore, and you haven't done anything to protect yourself, you're going to get it, too. "[Viruses] are out there in force and they're banging on everybody's door trying to get in."

"If there's any one thing that you wouldn't want to go without, it's anti-virus software," adds Lee. He suggests taking advantage of a free virus scan from McAfee or Symantec, and then purchasing their software to wipe out any existing infections and stave off new ones.

"Reinstall the software on your computer every six months," recommends Marco Peretti, chief technical officer for BeyondTrust, a Portsmouth, N.H.-based developer of security software. "You and your employees are picking up 'Trojan horses' that endanger your computer every time you access the Internet."

Of course, virus infection can often be prevented, Lee points out, without software of any kind. He suggests, for instance, deleting e-mail attachments from unknown senders and only accepting PDFs—which are immune to computer viruses—from known ones.

3. Spyware Protection

Hand in hand with anti-virus software is spyware protection, experts say.

"[Spyware] is looking at your stuff when you're typing it in and secretly sending that information to somebody else," Lee says.

Spyware—programs that are downloaded secretly to your computer—can hijack your hard drive and turn it into a conduit for identity theft and spam, compromising not only your own integrity, but also your customers' data.

"Spyware is easily fixed by understanding that Windows will never ask you, 'Do you want to make your computer faster?'" Lee says. He suggests avoiding pop-up windows—"Whatever you do," he says, "don't click on them"—and file-sharing software that's paid for by advertisers, who often attach spyware to the downloads they subsidize.

"Good spyware protection is available for free with a program such as Microsoft Windows Defender," Stein says.

4. Data Protection

Even if you survive spyware, your data may not be secure. To protect your valuable information—things like employees' social security numbers and customers' credit card numbers—store it on a server rather than a personal PC, says Stein.

"The server should be in a secure location, as well," he says. "All data should be backed up once a day, and the back-ups need to be kept secure also."

Of course, not everything can be kept on a server. If you store important information on your laptop or PC, you should take care to secure that information. Save confidential files to a thumb drive, for instance, and avoid transmitting important information over unsecured wireless networks.

Finally, and most importantly, protect your data with strong, secure passwords. A "strong password," according to Stein, is one that's changed quarterly, contains no words, includes both upper- and lower-case letters, has both symbols and numerals, and is between eight and 10 characters long.

"You'd never believe how many secure systems have users who have default or easy-to-guess passwords implemented—such as password, admin, abc123, etc.," he says.

5. IT Policies and Procedures

A final tool for strong computer security, according to Peretti, is a sound and structured set of IT policies. "Many small businesses start with anti-virus software, but then pay little attention to good security policies because the perception is that they'll be safe no matter what," he says.

That perception is wrong. Businesses should therefore define how company computers may and may not be used, Peretti says, as most security slip-ups happen when an employee misconfigures his or her machine or downloads unapproved software to its hard drive.

"Most of your danger is from your own employees," Gutman adds, "and by not being protected, your letting your machines become zombies—somebody else is controlling them."