

Do You Know Where Your Laptop Was Sleeping Last Night?

By

Raymond E. Muth, CPA, CISA, CISSP, CITP
President, BankLogic.Net, CPAs & Consultants

I was attending a seminar on Ethical Hacking (yes, that was the real title) when the presenter mentioned how he usually performed his external penetration testing scans from a hotel with broadband or wireless Internet access. While that was hardly a surprise what he said next did wake some of us up. "Sometimes I like to scan all the computers on the network in the hotel. You can't believe how many people come to these hotels with no personal firewalls or encryption on their laptops."

The tool this fellow used to access these laptops was free and widely available. Incidentally, the vast majority of tools used by the bad guys are not only free and easily downloaded, but they are also extremely effective. If you connect the dots, the presenter had access to almost any file on any of these unprotected laptops in the hotel.

Bank networks protect their servers and workstations by configuring a firewall to prevent intruders from hacking back into their systems via the company's internet connection. But once users leave the corporate buildings and connect to the web from home or a hotel room, their data is vulnerable to attack. Personal firewalls such as Norton and ZoneAlarm are an effective and inexpensive layer of security that takes only a few minutes to install. Windows XP comes with a personal firewall and in conjunction with service pack 2, the firewall is turned on automatically. But you should consult your IT support staff or IT vendor for the most effective personal firewall configuration for your bank's laptops.

It is important to consider that the vast majority of people who choose wireless connectivity for home use usually buy a router and plug it in without ever employing any of the security settings. You should assume that if you are permitting employees to go home with laptops, they will be using a connection that can be picked up by anyone. Therefore a personal firewall is a must.

In addition, there has been a strong push for core banking systems to make customer databases available in the Microsoft Office suite of products. This of course allows information to be more easily accessed, sorted, distributed and manipulated. Obviously sensitive customer information should never be loaded on a device that is not secure. Therefore, it is critical to get a handle on what information your employees have on their laptops. If sensitive information must reside on a laptop, encryption is vital. A program from pgp.com loads a virtual encrypted hard drive where sensitive files can be placed inside a virtual space that requires a strong password.

Finally, it is important to note that USB pen drives are small, inexpensive devices which can hold as much as 1 GB of information. That translates to a whole lot of customer information. These devices can be quickly inserted in and out of a USB port and information can walk out of your office in no time. This means that if a computer is left logged on, your outside vendors and clean-up crew have a very convenient way to grab customer information.

Send e-mail to raymuth@banklogic.net