



Business Plus Article – Jun 2006 Security on the Move

It's safe to say we are now in the age of the mobile worker. Many organizations are enjoying the benefits of a mobile workforce. Portable laptop computers have become much more affordable over the past few years and fast internet connectivity is ubiquitous. With a simple Virtual Private Network connection (VPN) to your network, employees stay in touch and are more productive while on the road. But along with the advantages of a mobile workforce come significant security concerns. Once a laptop leaves the company network, it immediately becomes a potential security threat unless properly managed. Previously in this column, we have talked about the need for stringent guidelines employed on a company network. In reality, even with such guidelines, without a similarly robust policy in place for remote users, it is simply a matter of time before your network is compromised.

So what can you do to minimize such risks? Let's look at a few basic steps to take to make a start:

Anti-Virus Software. Make sure the anti-virus software running on computers taken away from the office is as effective removed from the company network as it is when connected to it. It should be configured in such a way that it takes away any involvement from the user. It should keep itself up to date and deal with any virus threats without relying on any interaction from the user.

Anti-Spyware. Spyware is increasingly common and is taking over where viruses left off. Spyware can be as harmless as adding search engines to your web browser or be as malicious as completely hijacking your computer rendering it useless. Your anti-spyware software should have real-time component that continually scans for potential threats as well as an on-demand scan engine which can be scheduled to run at specified intervals.

Patch Management. We've previously talked at length about the need to keep our software up to date. Whether we do this via Windows Update, Windows Server Update Services or a third party product, remote machines should not be forgotten.

Firewall. A firewall sits between your computer and the Internet and acts like a barrier that protects your computer from hackers and other exploitive attacks. It goes without saying that remote users should have some kind of firewall protection. Whether it is a Windows based firewall or some kind of external firewall appliance, it should be inspecting both inbound and outbound network traffic.

Wireless Security. There are two major players in wireless security at the moment: WEP and WPA. WEP, or Wired Equivalency Privacy, is probably the most widely used at the moment. While it is comparatively weak when compared to WPA, or Wi-fi Protected Access, it is still strong enough to

withstand even the most persistent attacker if setup correctly. As a bare minimum, WEP should be enabled with a 128bit key although WPA is still preferable. Make sure you change the default passwords and SSID (the name you have given your wireless access point) on your access points.

Passwords. Educate your users. A password of simply “password” is no longer enough. A password should be at least 8 characters and contain a mixture of alpha-numeric (letters and numbers) characters. On portable devices such as laptops, consider a BIOS password that will require a password before allowing the computer to boot up, as well as the normal Windows password.

File Encryption. Consider using a file encryption utility. By encrypting a file, you are preventing any unauthorized access to it. Even with a strong password, if a laptop falls into the hands of an unauthorized user, they can easily circumvent security by removing the device’s hard drive or removable media, such as USB memory sticks, and inserting it in an unprotected device to gain access to the data. By encrypting data, this becomes infinitely more difficult.

By addressing the above issues, your network administrators can make your LAN a safer place as well as providing mobile workers with peace of mind. Remember, it’s better to close the stable door before the horse has bolted. To adequately protect your most important business asset - information – the time has come to expand your secured perimeter beyond the company network to include your mobile workers.

Matthew Smith
Raven Computers Ltd