Are You Indulging In Unprotected Wireless?

Author: Ian Kilpatrick - Chairman Wick Hill Group
Published: Friday, 03 September 2004 12:56 GMT

Wireless PCs and wireless laptops are being increasingly used in both business and the home. The reason for this marked trend is that wireless computers are easy to deploy, cheap and are usually simpler to manage than standard wired connections.

In the business world, smaller companies with two to two hundred and fifty users, find that wireless computing frees them from the conventional restrictions of cabling. Once a wireless device has been installed, new PCs or laptops can be added without the hassle of wiring them in.

Employees can still connect to the Internet, send and receive emails, and do all tasks they need to do. Moreover, they can do all this with greatly increased mobility. It’s a very attractive proposition.

For enterprises, wireless provides laptop users with convenience and mobility. They can use their wireless laptops in the office (often without the knowledge of management), from home, and of course when they’re on the move. When they’re out of the office, executives can work from one of the many wireless ‘hot spots’ springing up in places such as Starbucks or hotel chains.

For home users, wireless laptops let you connect to the Internet, without being physically tied to a connection point. More than one user can easily connect up from different locations in the house and you can have privacy from other family members when you need it. And, of course, you can easily connect to the office.

Unprotected wireless

Unfortunately, in the enthusiasm with which people have adopted wireless, the question of security has been seriously overlooked. There is a standard for security over wireless which is WEP 802.11b (Wireless Equivalent Privacy). However, this standard is both flawed and weak, being ineffective and easily broken.

It is also rarely implemented. This is because it is easier to set up wireless with the security not enabled. Once the wireless system is working, the security tends to remain switched off. This has been confirmed by recent surveys in London which showed that 67 percent of sites surveyed using wireless did not have security enabled. The same problem potentially exists with the new security standard WPA (Wi-Fi Protected Access).The default set-up configuration is again with the security not operating.

Some might ask what difference WEP’s insecurity or the absence of any security at all makes. The answer is ‘A lot more than you might think’. The whole concept of wireless is about broadcasting, which means that the information doesn’t just go to the wireless connection but is also available to anyone within broadcasting range.

Sadly, while you may believe that your near neighbours or neighbouring offices may have neither the will, interest nor technology skills to be interested in your wireless activity, that doesn’t mean you are secure.

There is a whole range of individuals and groups who have a deep and not always savoury interest in unprotected wireless users.

Some groups have a very active but essentially harmless interest in unprotected wireless, being concerned mainly with finding and identifying wireless sites. You've probably heard about some of these in the press Their activities have a name. ‘War driving’ is driving around looking for locations where wireless is being used and is not secured. It has many web sites devoted to it such as www.wardriving.com.

‘Warchalking’ is marking up street locations with special symbols to identify wireless locations. Again, many web sites are devoted to it (e.g. www.warchalking.org). There are even details online of where to find unprotected wireless sites in UK towns and cities.

As your wireless device broadcasts its address (SSID), it is extremely easy

As your wireless device broadcasts its address (SSID), it is extremely easy for anyone to do this – it can even be done with a PDA. If you're currently indulging in unprotected wireless broadcasting, it is quite possible that you're already on one or more list. In addition to these groups, there are those with a far from innocent interest in your wireless broadcasts.

But there's not much at risk

Unfortunately, this is totally wrong, even if all you ever do with your wireless PC is access harmless web sites from home. It's not just what you broadcast that's at risk, but everything else on your PC or laptop. So information such as passwords, bank details and any other personal data which you wouldn't want other people to know, are all accessible, as is any information on your wireless servers

And very worryingly, if your connection is used for illegal activity such as accessing illegal images on the Internet, you or your business could be held responsible, even if you have no idea who actually did it. This is because the activity will have been carried out from your address, using your connection,

If you have staff at work to whom you have provided wireless access, or more commonly who have provided themselves with wireless access from their laptops, the odds are that they haven't even enabled the weak, cursory WEP 'security' encryption.

As they are operating outside the normal company network and its protective measures, they are therefore not only broadcasting any information they are handling, but have opened up your network to anyone else who cares to look.

An obviously serious security weakness, negating all the effort you have put into making your systems secure.

Unprotected wireless use exposes companies and individuals to a wide range of security problems. These range from unauthorised use of your bandwidth through to the theft of confidential personal and company information held on your laptop, illegal use of your connections, and in the worse cases industrial espionage and fraud.

The CSI/FBI survey of 2003 shows once again that there are significant levels of hacking, system penetration, eavesdropping, sabotage, theft of proprietary information and insider abuse of company's computer systems.

Wireless looks like a very easy way to carry out many of these activities, given the ease of access and the low likelihood of detection.

Protecting yourself

With all of these risks and so few people protected against them, it would seem that wireless protection is either desperately expensive or incredibly difficult. However, this is not the case.

For normal landline communications, most companies today use encrypted VPNs (virtual private networks), most commonly to the IPSec standard. These are used to protect communications between two points, usually between a head office and branch office, suppliers or home workers. One solution to the inherent insecurity of wireless is to use IPSec encrypted VPNs for communications between the wireless user and the wireless access point (or company network).

Encrypted VPNs will create a secure connection between the wireless user and the VPN gateway of the company. This connection now hides your communications. The data on your PC is protected from prying eyes because the communication route for it is through the VPN. This method therefore not only protects and encrypts your wireless activity, but also prevents unauthorised wireless access to your PC or business servers by requiring authenticated VPNs for all wireless use.

If you are communicating with a supplier, customer or indeed head office, you have not only protected confidential data, you have also prevented your connections from being used to compromise their security.

Installing and implementing VPNs is more complex than using unprotected

Installing and implementing VPNs is more complex than using unprotected wireless, but is not beyond the skill set of PC literate individuals who need the benefits of protection. If you're looking to implement wireless VPNs, prime features you need to look for are

- ease of installation and use
- compliance with standards (802.11b is the one currently in widest circulation)
- capability to use a VPN (This latter feature is not as obvious as it sounds, because some "secure" wireless units have firewall functions but do not support VPNs).

Products such as the WatchGuard SOHO 6tc wireless (www.watchguard.com) support VPNs and also provide firewall functionality. Solutions of this nature are available from the low hundreds of pounds and can be deployed in home offices, small offices and wireless nodes in large enterprises. While there is a small performance impact through using VPNs, the increase in security is significant.

Safe rather than sorry

Wireless provides many benefits to business users, which include low cost, greater mobility and being able to alter desk layouts with the minimum of hassle. These benefits mean wireless is spreading rapidly. However, security breaches occurring through wireless use are also increasing, with consequent high costs.

It is both inexpensive and comparatively easy to secure yourself against broadcasting your secrets to anyone who is interested. The latest generation of wireless defence solutions means there is no longer any reason to participate in unprotected wireless.

Ian Kilpatrick is chairman of Wick Hill Group, a company specialising in secure infrastructure solutions for ebusiness.