Are you exposed to hackers?

In recent years, many organisations have embraced the use of wireless networks (commonly known as WiFi) in their computing environment.

This technology should not be confused with the wireless technologies used by mobile phone carriers.

The former allows employees to access their corporate network without cables in a transparent, fast and efficient way. However, wireless computer networks that are setup insecurely can have grave consequences for organisations.

WiFi networks are definitely revolutionary. Not so long ago, companies who wanted Internet and network access in a new office needed to hire professionals to install wiring and network wall jacks.

With WiFi, all that is needed is a small device (called a wireless access point) allowing wireless connections to the existing network. Within minutes, users can access their corporate network and the Internet, without cables, with their wireless enabled laptop.

Unfortunately, all this convenience can present huge risks without a proper setup.

In fact, wireless networks can have serious impacts on the overall security of networks and of course the data they contain.

To see how organisations are doing with regards to securing WiFi networks in Grand Cayman, a small test was performed. Within 10 minutes, equipped with a laptop and a free software tool, seventy wireless networks were identified. Out of these networks, 40 per cent did not use any form of encryption, thus making them attractive targets for hackers.

It is important to note that for this test, no networks were accessed; the networks were simply identified and not investigated further.

Possible consequences of insecure wireless networks are multiple and can be devastating.

First and foremost, a hacker could access a corporate network and steal, destroy or modify critical data.

What happens is that by accessing a network via a wireless device, the hacker bypasses the firewall and other security mechanisms, thus gaining direct access to the corporate network.

Also, users of an insecure wireless network could have passwords and sensitive documents captured by a hacker who has gained access to the network and is passively intercepting data.

In all fairness, some of the unencrypted wireless networks which were identified during the test could simply be guest networks.

These networks are setup in conference rooms for clients or guests of the company so they can check their email.

These can still be a risk even if they are completely separated from the corporate network. In fact, an unauthorized user could perform numerous actions which could expose the organization to unnecessary risk.

For example, the wireless network could be used to attack a government web site, the web site of a competitor or a well known eBusiness site. Also, the unauthorised user could use the open network to send out millions of spam e- mail messages.

In both of these cases, the organisation may get in trouble when the incident is traced back to its origin: them!

It is clear that many organisations in Cayman, like elsewhere in the world, need to increase their awareness to the fact that wireless computer networks are liabilities and can cause serious data confidentiality, availability and integrity issues.

Organisations must realise that a wireless networks is an extension of the corporate network. Unfortunately, the airwaves used by the wireless devices do not stop at the walls of a building and can be accessed from the outdoors, just like a cordless phone that still works in the backyard of a house.

So basically, an intruder who is in the parking lot or in an adjacent building could connect to the corporate network just as if he or she was physically sitting in premises of the organisation.

It gets worse, An employee can easily add a wireless device on a corporate network for convenience sake and unwillingly expose the whole network to hackers. Wireless devices are affordable and extremely easy to setup.

I have personally seen many networks that were exposed by an employee who did not realise the consequences of installing a wireless device on the corporate network.

There is good news.

A wireless network can be setup and configured to be secure.

These enhancements are mostly device configurations and selecting an appropriate location for the WiFi device on the network.

There are many resources available on the Internet and from hardware vendors to assist with securing these devices. Encryption and authentication methods should be used and frequently revised.

Finally, IT groups should regularly verify the presence of rogue wireless devices which may have been setup by employees.

I invite readers to contact me with any IT security related questions.

I will also be happy to meet with organisations that have IT security concerns and who wish to discuss them in a confidential manner. Please e- mail me at michoschumann@kpmg.ky or telephone on 949 4800.

The views and opinions are those of the author and do not necessarily represent the views and opinions of KPMG. All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity.

MANAGING INFORMATION RISK

by **Micho Schumann, Manager, IT Advisory, KPMG**