Wireless security? Are you throwing your money out the window

Mark Osborne explains why companies need to get their act together in protecting wireless networks and handheld devices, or become a statistic in the rise of drive-by hacking

1 Introduction

Have you seen that advert on the TV or at Cinema about mobile computing –

A professional young woman is surrounded by a noisy bunch of louts, shouting and having fun (Hurrah, my kinda job - where do I apply). Frustrated, She can neither get them to shut up nor can she concentrate on finishing the vital report she is trying to complete. Undeterred, she takes her top of the range laptop and without the slightest word goes to sit in the stairwell to complete her report. The last shot shows here triumphantly handing what can only be a masterful report to her boss whilst the voiceover claims that it was all possible because of the wireless network card.

Is it really such a good idea to broadcast our corporate secrets on the airwaves – if so why did we spend so much money in the past, locking our servers away & securing our networks. The reality is nothing is that simple, and your corporation complete with trite stairwell sitting yuppie bint could be losing competitive advantage – Effectively throwing your companies profits out the window.

1.1 The FACTS

In a recent Global Information Security Survey conducted by KPMG, it came to light that 43% of organisations had either implemented some form of wireless network or were planning to. But of those who have fully implemented a wireless network, 38% do not use virtual private networking or other security technology to protect the data flowing over it. Research we are currently conducting (due for release in autumn) suggest the threat is greater than most believe.

Given the publicity over Wireless Lan (WLAN) security vulnerabilities and, WEP (Wired Equivalent Privacy) poor strength, this indicates that future incidents are evitable.

1.2 Drive-by hacking

This failure to address wireless security issues is exposing companies to the risks of drive-by hacking. So what is War-driving or drive-by hacking? Hackers ever keen to try new techniques have discovered that the radio signals from Wlans often extend by hundreds of feet past the building perimeter. With an ordinary WLAN network card and freely available scanning software, they can easily detect networks by patrolling commercial districts and establish if they are able to connect to them. And as our survey points highlights, in most cases they will succeed.

2 Three steps to Safe Wlans

Many people err on the side of caution and make the logical assumption that if they do not use WLAN technology, no further action would be required to maintain security. Unfortunately, such a simplistic strategy is prone to failure – Many of the security problems we have seen arise from wireless equipment informally installed without the knowledge of the organisations IT department. Many end-users have the technical ability to install/configure these user-friendly, plug&play devices without any assistance from the in-house network gurus. However, it is unlikely that the same end-user would fully appreciate that by doing so he created a huge backdoor into the corporate networks circumventing the organisations security and possibly causing the companies most secret data to be broadcast over the airways to be received by any enterprising listener.

Step1: So as a first step whether you intend to take advantage of the flexibility of mobile Ethernet or not, prudent IT management should ensure that the risks of unauthorised installations are included their security awareness programme. Additionally, they should confirm that no unauthorised installations have taken place by regular scanning.

Step2: If you do feel there is a business advantage to using WLANs, the next step is do a quick risk analysis to determine the security needed. Many risk analysis techniques are labour intensive and resemble a job creation scheme. This is definitely **NOT** what we are suggesting. The objective here is to **save** money and assess the importance of the data that is exposed. For example many companies use WLANs to provide hot-spots to allow mobile sales staff access to printing and web-browsing facilities. If this is all that is required, it may be a case that only a basic security solution is required – this may involve no extra cost.

For example, lets examine a case we dealt with in the fast moving world of journalism. A head-line story was believed to have some financial value for upto 59 minutes until the

www.loud-fat-bloke.co.uk

next hourly bulletin but after that the information would be in the public domain. In such a case, the confidentiality of data only had to be provided for 59 minutes - even the use of the much maligned and flawed WEP could be safely employed. But when you make an assessment like this please, don't forget your use of passwords. Most of us use them and often encryption is employed simply to protect them, as typically they only change monthly. Fortunately, in this case, one-time password tokens and MAC based access control were in use. In short, the risk analysis allows you to focus your security efforts where they are most needed.

Step3: Implement and test – Most WLAN implementations require full access to the corporate LAN and in such a case, unfortunately, the built-in security mechanisms of 802.11 coupled with the mediums ability to transcend physical boundaries (even in the 21st century it is surprising how much we still rely on doors, locks, walls and wires) means a technical complex solution may be needed. Typically when providing a full Lan2WLAN connection you should consider the following;

VPN – A virtual private network (or other suitable encryption technology) will almost certainly be required to ensure that those business plan AND your passwords are safely encrypted – protected from those who would eaves drop.

Strong-authenticate – passwords are acceptable within the confines of buildings and internal network. However, WLANs are external networks and just as easy to access as the internet or the phone network. In such environments malicious hackers use highly effective programs like Brutus to make short work of password-based defences. A good solution should be based on two factor token authenticator or Digital Certificates. This should integrated into your VPN solution using Hybrid-Ike.

Flexible-perimeter – These days with VPNs, Extranets and ASPs it is hard to tell where your network ends and the outside world begins. However, even if you are implementing VPNs and Strong Authentication, there are definite advantages to installing your Access points (AP) in front of a firewall. Often this can be done using your existing RAS infrastructure and capitalise on your existing monitoring regime.

WLAN parameters – Sensible precautions like changing your SSID (network name) to something that isn't enticing to hackers is advisable, as is limiting the Aps response to general broadcast probes (if the ap can be configured as such). Also change the default device passwords and community strings.