Feature:SECURING WIRELESS, REMOTE AND MOBILE COMPUTING - SOME QUICK FIXES

Submitted by: Nuvias (Wick Hill)
Friday, 30 June 2006

Dear Editor,

Following is a feature for publication entitled:
SECURING WIRELESS, REMOTE AND MOBILE COMPUTING - SOME QUICK FIXES

Please feel free to publish this, on proviso Ian Kilpatrick, chairman of Wick Hill Group, is acknowledged as the writer.

Best wishes
Annabelle Brown
PR for Wick Hill

SECURING WIRELESS, REMOTE AND MOBILE COMPUTING - SOME QUICK FIXES

600 words

By Ian Kilpatrick, chairman of Wick Hill Group, specialists in secure infrastructure solutions for e-business

The rapid growth of wireless, remote and mobile computing is creating a significant increase in the risks that organisations face. All the indications are that this growth will continue, and indeed accelerate. It is clearly time to review what actions are required to manage access risks from these forms of computing. Fortunately, there are some quick fixes that are available.

In an ideal world, the starting point would be risk assessment and management. This is a fundamental component of any wireless and mobile deployment. It will ensure that security is factored in at the beginning of a project and that everyone involved is aware of the risks. All security policies should be reviewed to make sure that they reflect current realities.

However, in many cases, the move from inside to outside the computer network perimeter has not been accompanied by either risk assessment and management, or by the education of the management, staff and users involved.

In an environment with ongoing mobile computer access, attempting to “backfill” security is going to be difficult and subject to active or passive resistance from users – and much more expensive than getting it right in the first place. A bite at a time is the best approach in this situation, and there are some quick fixes that will make it an easier case to sell to all involved.

* Passwords and authentication

Static passwords are woefully inadequate for remote and mobile computer users, with huge identity theft

risks (particularly for wireless). The answer is to deploy strong two- factor authentication. Companies such as VASCO provide low-cost, token-based solutions that can be easily deployed for remote users.

* SSL VPNs

Consider using encrypted secure sockets layer (SSL) VPNs, alongside or instead of IPsec VPNs, as SSL can provide lower cost, easier to manage connections for large numbers of remote users. This is a growing area and there are a wide range of solutions from WatchGuard, Citrix, AEP, etc.

* Regular Updating

Make sure that users regularly update anti-virus and firewall software. Failure to do so, alongside password and unauthorised software related issues, makes up the majority of remote help desk problems for organisations.

* Wireless

Ensure that all traffic is over VPNs and is encrypted. Don’t use Wired Equivalent Privacy (WEP) for encryption because it is poor, insecure and weak. Use WPA or WPA2 (also known as 802.11i) and ensure that users always operate with it switched on - the default is with it switched off.

If you have remote wireless LANs, ensure that the service set ID (SSID) is changed from the default and is secured. Don’t change it to something blindingly obvious like your company name (or “control tower”, as seen by startled laptop users at a US airport).

Implement media access control (MAC) filtering. A MAC address is a physical address, so if you restrict access to devices whose address you have authorised, you can eliminate many ID theft issues. Another variation of this is device authentication, where the device authenticates itself to the network. Solutions are available from companies such as Phoenix Technologies, etc.

Also ensure your users have a wireless firewall/VPN to protect them and to manage encrypted VPNs from the wireless device. Companies such as WatchGuard and Check Point provide centrally manageable solutions in this area.

Bear in mind that many cheaper remote firewalls are incapable of dealing with application level attacks. A key requirement for remote firewalls, wireless or static, is to be able to deal with current and future threats, which include packet and, increasingly, application level attacks. All of these measures should greatly improve your mobile computing security with the minimum of fuss and resistance from staff.

ENDS

June 30th 06

For further press information, please contact Annabelle Brown on 0191 252 8548, email a_brown@dial.pipex.com. For reader queries, please contact Wick Hill on 01483 227600, web

www.wickhill.com. Pic of Ian Kilpatrick available from www.prshots.com (search for Wick Hill)

Bio – Ian Kilpatrick

Ian Kilpatrick is chairman of Wick Hill Group plc, based in Woking, Surrey. Wick Hill specialise in secure infrastructure solutions for ebusiness. Kilpatrick has been involved with the Group for 30 years and is the moving force behind its dynamic growth. Wick Hill is an international organisation supplying most of the Time Top 1000 companies through a network of accredited resellers.

Kilpatrick has an in-depth experience of computing with a strong vision of the future in IT. He looks at computing from a business point-of-view and his approach reflects his philosophy that business benefits and ease-of-use are key factors in IT. He has had numerous articles published in the UK and overseas press, as well as being a regular speaker at IT exhibitions.